NOW IS THE TIME FOR EXPANDED REMEDIES IN INFORMATION AND COMMUNICATION TECHNOLOGIES, ESPECIALLY SOCIAL MEDIA

Michael Losavio[*]

INTRODUCTION

An old maxim is there is no right without a remedy.[1] But an autonomous person may surrender her or his rights so that there

[*] Michael Martin Losavio, Associate Professor, Department of Criminal Justice, University of Louisville, USA.

[1] In *Marbury v. Madison*, 5 U.S. (1 Cranch) 137 (1803), the Supreme Court cited Blackstone: "I am next to consider such injuries as are cognizable by the Courts of common law. And herein I shall for the present only remark that all possible injuries whatsoever that did not fall within the exclusive cognizance of either the ecclesiastical, military, or maritime tribunals are, for that very reason, within the cognizance of the common law courts of justice, for it is a settled and invariable principle in the laws of

is no remedy available for injury, absent some provision of law that bars such a waiver. This ranges from a felon on trial entering a plea of guilt and waiving any right to a trial before a jury to a consumer accepting significant limits on remedies for product failure.

This latter waiver/limitation on remedies is of particular concern within the realm of computing and information/communications technologies. Without liability for injuries caused by their products, computing and ICT may have less incentive to engineer safety first into their products. Reliability should always be a concern to protect the market for a product, but other factors may give rapid innovation precedence over reliability or safety concerns. One tech company's motto for a time was "move fast and break things" to encourage innovation.[2]

Similarly, efforts to encourage technical innovation may engender statutory provisions that offer immunity to creators of technical systems to swiftly develop new technologies, even when people may be injured by them. A prominent example is Section 230 of the Communications Decency Act, designed to encourage the development of online systems for the exchange of information through statutory immunity for third-party content on their systems.[3] The Congressional findings preliminary to the statutory language expressly stated that "[t]he Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity . . . to the benefit of all Americans, with a minimum of government regulation."[4] It was the policy of the United States to promote the continued development of these systems, to preserve the vibrant and competitive free market" of the Internet "unfettered by

England that every right, when withheld, must have a remedy, and every injury its proper redress." 3 WILLIAM BLACKSTONE, COMMENTARIES *109.

[2] In a letter to potential investors in Facebook's initial IPO, Mark Zuckerberg noted that core values include "move fast": "Move fast and break things." *Mark Zuckerberg's Letter to Investors: 'The Hacker Way'*, WIRED (Feb. 1, 2012, at 18:35 CT), https://www.wired.com/2012/02/zuck-letter/ [https://perma.cc/E9CL-86U9] ("The idea is that if you never break anything, you're probably not moving fast enough.").

[3] 47 U.S.C. § 230.

[4] *Id.* § 230(a)(3)-(4).

Federal or State Regulation."[5] No provider nor user of these systems would be treated as a publisher or speaker of content provided by a third party nor face civil liability due to good faith efforts to filter out objectional material; state laws to the contrary were preempted.[6] This gave significant immunity to operators of such systems for the content posted by third parties. As discussed below, that immunity may be and has been restricted by statute; this was done with the FOSTA/SESTA legislations relating to issues of sexual and child exploitation.

With limited or no remedies, either by contract or statute, rights that may apply in other areas are absent or unavailable in these areas of activity. An important issue is whether or not these rights will be restored by limits on contractual waiver or statutory immunity to avoid liability for injury. The technical and social facts that first justified sheltering certain technologies have changed with time to weaken the reasons and justifications for such protections. People should be empowered that they may assert their rights to be free of injury from technologies; liability shields should be limited or removed to hold information and communications technology operators accountable for the injuries caused by their systems.

I. THE SURRENDER OF RIGHTS VIA END USER LICENSE AGREEMENTS

From the beginning of popular and widespread distribution of computing systems, especially software and systems online, many authors and vendors of those systems required a user to agree to a prior licensing agreement. Many of these, styled as an End User License Agreement ("EULA") for the system or software, must be agreed to by the user before they could use the system or software. These licenses and EULAs often had limitations of liability provisions relating to the failure of the system or software that limit damage, often to only the cost of the software. When a small business crashes into bankruptcy as its accounting software crashes, they would be left to only claim the cost of that software, not the value of the business destroyed. These licensing

[5] *Id.* § 230(b).
[6] *Id.* § 230(d).

agreements are also used to control other aspects of system usage, such as prohibitions on particular uses of the software and violations of intellectual property.

A hallmark discussion of a person's right to waive their rights and responsibilities was detailed in *ProCD, Inc. v. Zeidenberg*, an early case involving the incorporation of a "shrinkwrap license" within the container of the medium holding the software.[7] In the facts surrounding that case, ProCD's database of telephone numbers, supposedly compiled at great expense, was acquired off the shelf and harvested by Zeidenberg to provide online access to those same telephone numbers. Zeidenberg did this despite a licensing agreement that prohibited such action, which he asserted he never saw or read. The United States Court of Appeals for the Seventh Circuit gave that argument short shrift, noting commercial practice holds a purchaser to provisions they did not read in such circumstances.

While other courts of appeals in other circuits in the United States have been slightly more flexible as to these agreements, the end result is that a consumer is bound by them whether they read the agreement or not.

And most consumers simply click "agree" and move on to access the system without reading the agreement. For example, the software vendor GameStation on April Fools' Day in 2010 included a provision that by agreeing to the EULA, the consumer also agreed to surrender their soul to the company:

> By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non-transferable option to claim, for now and for ever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorised minions.[8]

---

[7] *See generally* ProCD, Inc. v Zeidenberg, 86 F.3d 1447 (7th Cir. 1996).

[8] Kevin D. Williamson, *Read the Fine Print*, NAT'L REV. (Apr. 20, 2010, at 20:43 CT), https://www.nationalreview.com/corner/read-fine-print-kevin-d-williamson/ [https://perma.cc/U6PF-LMLG].

Although there was an opt-out button, the vast majority of the 7500 people accessing the system that day proceeded to agree to the EULA without opting out of its provisions despite the risk to their post-life spiritual health.[9]

Where provisions of EULA agreements become too onerous and conflict with other consumer law provisions, those provisions may be voided. That may risk the possibility of voiding the entire agreement and the protections it gives the software maker. But the typical provisions for waiver of any liability for injury by use of the system have been upheld by U.S. courts and continue to be a core component of EULAs.

In the early days of software development, such provisions, though challenged, were upheld as part of the contract process. A user did not have to agree to them, though they could not then use the software. Given the centrality and pervasiveness of such systems to contemporary life, EULAs should not continue to receive complete deference in the face of injury to others.

The voiding of such agreements for abusive terms is not sufficient to protect users, especially consumers, given the ubiquitous nature of those systems. This lack of protection is heightened by the distribution of consumer systems to consumers who have not been trained in system operations, nor the law, in order to understand their risks.

Simple requirements for reliability testing and disclosure before a EULA can be deemed enforceable can contribute to improved software safety. These requirements introduce both legal liability and market accountability as incentives for better, tested software. This can range from system performance reliability to system cyber security. The end result protects everyone, especially as cyber security is a growing problem where a flaw in an application is the doorway to mischief across the system in which it is installed and, potentially, all the other computing systems with which it may connect or interact.

[9] Peter Steven Ho, *Software Licenses: Selling Your Soul*, MEDIUM (Sep. 13, 2021), https://peterstevenho.medium.com/software-licences-selling-your-soul-553c3f05e559 [https://perma.cc/HGM8-WPDJ].

II. IMMUNITY PROVISIONS—COMMUNICATIONS DECENCY ACT SECTION 230

Online systems are protected under the First Amendment to the U.S. Constitution.[10] That only protects them from some, but not all, liability where their systems are used to injure others directly or indirectly through use of their systems by third parties. To assure immunity from third-party conduct, particularly for an online system that wishes to edit, censor, or otherwise limit third-party content and to promote the development of online systems, as discussed above, the U.S. Communications Decency Act Section 230[11] gave those systems immunity from liability for evil content posted by third parties that may be delivered via those systems.[12] Under the technology of that time, it was either impossible or prohibitively expensive to vet all content posted by third parties. Section 230 extended immunity to online systems similar to those given under common law to libraries and bookstores for their broad content.

This statutory immunity has been limited or removed by legislative action in relation to particular types of content. This has been done in human trafficking, commercial sex services, and child sexual exploitation via these systems under the FOSTA-SESTA amendments to Section 230. These amendments were made in 2017, twenty years after the passage of Section 230 and after extensive exploitation of people, especially children, through the use of online systems by malicious actors.[13] Such revisions to

---

[10] "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. amend. I.

[11] Communications Decency Act of 1996, 47 U.S.C. § 230 (providing a safe harbor immunity to providers of an "interactive computer service" that may republish content from third parties).

[12] *See generally* Gonzalez v. Google LLC, 598 U.S. 617 (2023); Twitter, Inc. v. Taamneh, 598 U.S. 471 (2023).

[13] *See* Allow States and Victims to Fight Online Sex Trafficking & Stop Enabling Sex Traffickers Act (FOSTA-SESTA), Pub. L. 115-164, 132 Stat. 1253 (2018); *Unconventional Wisdom: Research Shakes Up Assumptions About Sex Trafficking Clues in Online Escort Ads*, NAT'L INST. OF JUST. (May 8, 2024), https://nij.ojp.gov/topics/articles/unconventional-wisdom-research-shakes-assumptions-about-sex-trafficking-clues [https://perma.cc/5A73-V3CS].

ICS immunity may expand in the future, possibly with unexpected or undesired impact. Content moderation removing immunity for commercial sex services may have unintended harmful effects, such as reduced safety for the service providers.[14] The Internet "puts every user close to all the evils of which we could possibly conceive,"[15] such that continued exploitation of others via these systems may lead to further legislative removal of safe harbors of immunity. Such exposure to liability may incentivize ICS/OCS online services to embrace protective technologies or counter-lobby legislative bodies as to the technical impracticality of effective protective systems.

III. CASELAW INTERPRETATIONS AND LIMITS ON IMMUNITY

The mixed legal regime of the United States includes judicial action as a means of modifying legal liability or legal clarification, including that relating to Section 230 immunity for ICS/OCS operations. Early judicial challenges to Section 230 immunity for defamation by third parties posted on various ICS/OCS systems failed, with courts citing the immunity provided by Section 230. As the United States Court of Appeals for the Fourth Circuit held: "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."[16] A series of cases followed relating to third-party emails, third-party false postings, third-party messages, and other third-party misconduct that affirmed the immunity Section 230 provides for online services applies to content posted by third parties.[17]

There is some questioning of the effectiveness of the FOSTA-SESTA Acts and indicating negative impacts from this legislation. *See, e.g.*, Ayelet Gordon-Tapiero, Yotam Kaplan & Gideon Parchomovsky, *Deepfake Liability*, 104 N.C. L. REV. 377 (2026).

[14] NAT'L INST. OF JUST., *supra* note 13.

[15] Michael Losavio, *AI Accountability & Social-Technical Solutions for the Regulation of Internet Free Speech*, 55 U. PAC. L. REV. 243, 245 (2024).

[16] Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998).

[17] *See* Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003); Gentry v. eBay, Inc., 99 Cal. App. 4th 816 (2002); Kathleen R. v. City of Livermore, 87 Cal. App. 4th 684 (2001); Universal Commc'ns Sys., Inc. v. Lycos, Inc., 478 F.3d 413 (1st Cir. 2007) (holding that a message board was not liable for users' messages); Schneider v. Amazon.com, Inc., 31 P.3d 37, 39 (Wash.

An intent of Section 230 was to permit ISCs to censor material posted by others without becoming liable for that content, whether or not censored. This came in the aftermath of the 1995 *Stratton Oakmont, Inc. v. Prodigy Services Co.*[18] defamation case,[19] which indicated to online ICS/OCS operations that *any* censorship or editing of content made the ICS/OCS liable for all third-party content, regardless of the practicality of content control. This was interpreted that any editing by the ICS/OCS would make it liable, such that they would do no curation of content no matter how vile; Section 230 protected an ICS/OCS from that liability if they acted to protect their users from improper or dangerous content.

Murders by terrorist groups using online content services led to new challenges to Section 230 immunity. Two judicial challenges to Section 230 failed even as they involved horrific outcomes. In *Twitter, Inc. v. Taamneh*, the family of a person murdered in a terrorist attack by the Islamic State of Syria and Iraq ("ISIS") sued, alleging that social-media companies aided and abetted ISIS in its terrorist attack on the Reina nightclub where ISIS had used those services.[20] But the Supreme Court held that those allegations did not detail a sufficient connection between the social media company's conduct and that of ISIS and failed to state a claim under the U.S. Antiterrorism Act;[21] with no cause of action, Section 230 immunity was not invoked to protect Twitter and other ICS/OCS operations. [22]

Taamneh was paralleled by the Supreme Court case of *Gonzalez v. Google LLC*[23] consolidated with it. The family of Nohemi Gonzales, killed in a nightclub bombing by ISIS, sued Google for aiding and abetting and conspiring with the Islamic

---

Ct. App. 2001); Doe v. Am. Online, 783 So. 2d 1010, 1013-17 (Fla. 2001), *cert. denied*, 122 S. Ct. 208 (2000).

[18] Stratton Oakmont, Inc. v Prodigy Servs. Co., No. 0031063, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

[19] Ironically, the allegedly defamatory allegations against Stratton Oakmont were followed well after the *Prodigy* case with the criminal convictions of several of its executives, its closure in 1996, and Martin Scorsese's film THE WOLF OF WALL STREET, Amazon Prime (Red Granite Pictures 2013).

[20] *See generally* Twitter, Inc. v. Taamneh, 598 U.S. 471 (2023).

[21] 18 U.S.C. § 2333(d)(2).

[22] *Twitter, Inc.*, 598 U.S. at 498-507.

[23] 598 U.S. 617 (2023).

State of Syria and Iraq. The plaintiffs asserted that Google had secondary liability via the use by ISIS supporters of its advertiser-supported YouTube system operated by Google. The case was dismissed by the Supreme Court for failure to state a claim, per the Supreme Court ruling in *Taamneh*,[24] but did not address the issues of secondary liability.

But Justice Jackson's concurrence in *Taamneh* noted the limited and narrow scope of the ruling and presciently noted that "[o]ther cases presenting *different allegations and different records* may lead to different conclusions."[25] This indicated that the immunity online operators enjoyed might not protect them in cases where different technical facts applied to their operations and content provision.

A greater causal connection between *what the social media company did*, even while serving up third party content, and the resulting injury, may overcome any claimed immunity under Section 230. This causal connection may be strengthened by the increased use of powerful algorithmic systems for both serving and directing that content to particular people. This connection also concerns social media's ability *to not direct such content to particular persons*, especially to vulnerable people such as children or those manifesting cognitive issues. That there was no intention on the part of the social media service does not change the injury that may have been caused by its conduct. As *Taamneh* and *Gonzales* show, that injury can be the death of the innocent.

---

[24] 598 U.S. 471 (2023).

[25] *Id.* at 507 (Jackson, J., concurring) (emphasis added) ("I join the opinion of the Court with the understanding that today's decisions are narrow in important respects. In this case and its companion, *Gonzalez v. Google,* 598 U. S. 617 (2023) (per curiam), the Court has applied 18 U.S.C. §2333(d)(2) to two closely related complaints, filed by the same counsel. Both cases came to this Court at the motion to-dismiss stage, with no factual record. And the Court's view of the facts—including its characterizations of the social-media platforms and algorithms at issue—properly rests on the particular allegations in those complaints. Other cases presenting different allegations and different records may lead to different conclusions.").

IV. WHEN ONLINE CONTENT SERVICES ACTS BECOME THEIR OWN EXPRESSIVE ACTIVITY

With *Anderson v. TikTok, Inc.*, [26] such a causal connection led the United States Court of Appeals for the Third Circuit to overrule the trial court's grant of a motion to dismiss and remand back to permit the plaintiffs to proceed on claims that included strict product liability and negligence. Those claims dealt with another horrific outcome, the asphyxiation death of Nylah, a ten-year old girl, after she did the "Blackout Challenge" asphyxiation activity from a video served up to her by TikTok's algorithmic recommender system.

TikTok sent the video to Nylah's "For You Page" ("FYP") due to its recommender system tagging it of interest to Nylah.[27] The Court of Appeals noted the "Blackout Challenge . . . encourages users to choke themselves with belts, purse strings, or anything similar until passing out," record it on video, and post it.[28] The underlying facts alleged were that TikTok "was aware of the Blackout Challenge," let users post videos of their doing the Challenge, and "recommended and promoted Blackout Challenge videos to minors' FYPs through its algorithm, including at least one such video to Nylah's FYP, which resulted in her death."[29]

Initially, the district court dismissed the case pursuant to the immunity of 230 of the CDA, which protects Internet interactive computer services ("ICS") from suit due to "information provided by another information content provider."[30] But the U.S. Court of Appeals noted Sec. 230 did *not* immunize from suit an ICS if they are sued for their own expressive activity or content (i.e. first-party speech).

The Third Circuit cited the 2024 U.S. Supreme Court's ruling in *Moody v. NetChoice, LLC*,[31] that curation of third party content to present via algorithm by an ICS is its own "expressive product"

---

[26] *See generally* Anderson v. TikTok, Inc., 116 F.4th 180 (3d Cir. 2024).
[27] *Id.* at 183.
[28] *Id.* at 182.
[29] *Id.*
[30] Communications Decency Act § 239, 47 U.S.C. § 230.
[31] Moody v. NetChoice, LLC, 603 U.S. 707, 716-17 (2024).

subject to First Amendment protection.[32] The *Moody* Court noted that a platform's standards or preferences, encoded in the algorithm's choices, might determine whether or not the algorithmic output, such as recommended content, was itself expressive content or simply third-party speech passed on to others with no expressive action by the ICS.

Section 230 was meant to protect ICSs from censoring material posted by others, but not the expressive activities of the ICSs themselves. The curation and direction by algorithmic recommender systems used to keep users engaged with the system were expressive activities by TikTok, for which they may be held accountable. The Third Circuit noted that a more traditional use of search features might have changed its holding: "Had Nylah viewed a Blackout Challenge video through TikTok's search function, rather than through her FYP, then TikTok may be viewed more like a repository of third-party content than an affirmative promoter of such content."[33] As TikTok had "affirmative[ly] promoted" through its FYP algorithmic recommender system,[34] it could not invoke Section 230 immunity to shield it from possible liability for Nylah's death.

Anderson establishes that the advances in commerce and marketing by online services make more and more of their actions their own expressive activity. For these actions, those services do not have the benefit of Section 230 immunity. They must prepare to be held accountable and must act immediately to protect their users by not serving up harmful content to them.

V. EVOLVING LIABILITY FRAMEWORKS

Shackelford et al. note efforts by nations to reform software liability, such as the European Union's Product Liability Directive to include software and injuries it may cause.[35] They suggest three potential avenues of effective liability for software products:

---

[32] *Moody*, 603 U.S. *passim*. The *Moody* Court did not address the issue of the impact of different algorithms as expressive activity, including those that "respond solely to how users act online." *Id.* at 736 n.5.

[33] *Anderson*, 116 F.4th at 184 n.12.

[34] *See id.*

[35] *See generally* Scott Shackelford et al., *Moving Slow and Fixing Things*, 100 IND. L.J. 1611 (2025).

> 1. Extending Products Liability to Include Cybersecurity Failings . . .
>
> 2. Adopting a "Secure-by-Design" Approach [, and] . . .
>
> 3. Enhancing Transparency and Accountability Through Regulatory Frameworks[.][36]

They further note the failure of "reactive cybersecurity" to protect systems and the need for new legal and policy tools to expand accountability for software and software systems;[37] these tools will range from contract terms to insurance/tax provision to state, national, and international laws and treaties to better assure accountability, with clear rules of products liability applicable to software. The EU's Cyber Resilience Act mandates cybersecurity requirements in design and sets out a liability regime, with developers required to run cybersecurity risk assessments and maintain security updates for up to five years; failure to do so risks severe financial penalties.[38]

A EULA may be found unenforceable due to unconscionable terms or violation of public policy, although they generally are upheld.[39] Potential avenues of further challenge may be for anticompetitive behavior in violation of statutes seeking to preserve and promote competition.[40] But statutory limits on the limitation of liability for EULAs may be necessary. The expansion of consumer protections against unfair trade practices as authorized for the U.S. Federal Trade Commission may be needed

---

[36] *Id.* at 1614-15.

[37] *Id.* at 1616-19.

[38] *See generally* Council Regulation 2024/2847 of Oct. 23, 2024, Cyber Resilience Act, 2024 O.J. (L 2847) 1. After September 11, 2026, "reporting obligations concerning actively exploited vulnerabilities and severe incidents having an impact on the security of products with digital element" come into force; full compliance applies after December 11, 2027. *Id.*

[39] *See, e.g.*, Bragg v. Linden Rsch., Inc., 487 F. Supp. 2d 593, 611 (E.D. Pa. 2007) (video game ToS included an arbitration provision that was deemed unenforceable due to procedural unconscionability); Reina Shinohara, Note, *Avatars and Derivative Works: Harmonizing the Interests of Creators and Consumers*, 73 HASTINGS L.J. 919 (2022).

[40] William Davis, *CUDA and the Walled Garden: How the Relationship Between Nvidia's Software and Hardware Violates the Sherman Act*, 8 BUS. & FIN. L. REV. 64 (2025).

to police EULA terms and content and enforcement as to protect all users.[41]

VI. LIMITS TO AMERICAN FREE SPEECH ABSOLUTISM

OCS may argue that whatever their expressive activities may be, they are protected under the First Amendment to the U.S. Constitution. But free speech protections are balanced with the nature of the interests it puts at risk. And different limitations on free expression are found among the many nations of the world. It is useful to examine these issues under U.S. law as it is the most solicitous of free expression, but even those protections for free expression are not absolute. Regulation can be implemented as needed to effectively protect a compelling interest with the least limitations on speech. The harm of the speech against the harm of its suppression must be weighed. Regulation must demonstrate that there is, in fact, an effective means of restriction and control. The early challenge to limit online speech was that there were no effective means for filtering content for children that would not impair the speech rights of adults.[42] That may no longer be true.

CONCLUSION

Changes in the power, reach, and abilities of software system developers and online technologies have created new and powerful challenges to those who use them. Heightened abilities for software testing and training make the failure to test, train, and warn users unjustified. The ability of online services to monetize their advertising and content provision has greatly expanded, especially with the implementation of algorithmic systems such as machine learning and artificial intelligence. This includes the benefits of content tailoring, editing, and direction to enhance the value of those content services to their users. On the other hand, those same new technical abilities of online services expand their ability to offer protection and filtering services to shield their

---

[41] Consumer Protection Act, 15 U.S.C. §§ 41-58.

[42] *See generally* Am. C.L. Union v. Reno, 217 F.3d 162 (3d Cir. 2000). For content-related regulation of speech, there must be a compelling interest at stake, an effective regulation, and no less strict avenues available to protect that compelling interest. Speech deemed not protected speech, such as obscenity and defamation, receives no protection.

users from exploitation and misdirection. This is especially important to protect their most vulnerable users, such as children who have used these systems, as well as the elderly who are new to the online world.

The excuses for shielding software/system developers and online services for bad outcomes to those who use them are greatly weakened. It is time for our societies to consider rendering those shields unnecessary, too dangerous to be allowed to continue, and hold software and software systems responsible for their actions.