DOI 10.5817/MUJLT2024-1-5

ONLINE PLATFORMS AND LEGAL RESPONSIBILITY: A CONTEMPORARY PERSPECTIVE IN VIEW OF THE RECENT U.S. DEVELOPMENTS

by

GERGELY GOSZTONYI * FERENC GERGELY LENDVAI †

This paper critically examines the relevance of Section 230 of the Communications Decency Act in the context of recent United States Supreme Court rulings, specifically Twitter v. Taamneh and Gonzalez v. Google. The Supreme Court ruled in 2023 that determining the extent of CDA230's immunity lies with legislators, not the judiciary. This study explores the potential liability of algorithms in supporting terrorism and the implications for European regulations under the Digital Services Act. Findings indicate that while CDA230 has fostered internet growth, it also challenges content regulation. The United States approach contrasts with the European Union's more explicit service provider responsibilities, suggesting a need for legislative updates to balance free expression with the control of harmful content.

KEY WORDS

US, SCOTUS, CDA, Internet, Liability, Google, Twitter

* Habil. Associate Professor of Law, ELTE Law School, Budapest. He is supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and the ÚNKP-23-5 New National Excellence Program of the Ministry for Culture and Innovation from the source of the National Research, Development and Innovation Fund

† PhD Candidate, Pázmány Péter Catholic University, Budapest. He is supported by the Rosztoczy Foundation and the ÚNKP-23-3 New National Excellence Program of the Ministry for Culture and Innovation from the source of the National Research, Development and Innovation Fund, lendvaigergely@me.com.

"We really don't know about these things. You know, these are not like the nine greatest experts on the internet."[1]
(Elena Kagan, Justice of the Supreme Court of the United States of America, 2023)

1. LIABILITY FOR INTERNET CONTENT IN THE UNITED STATES OF AMERICA

In the context of the nascent Internet in the 1990s in the United States (hereinafter: U.S.), based on early court practice,[2] many online platforms asked themselves whether it was worth moderating the uploaded content since if they did not do so, they were not a publisher but merely a distributor and were exempt from liability. However, this contradicted the need to curb the spread of problematic content on the Internet, as the lack of law and liability would have perpetuated the Wild West (or, in Alfred C. Yen's words, "western frontier"[3]). This dilemma has been resolved by an amendment to the U.S. Telecommunications Act, as was proposed by Republican Chris Cox and Democrat Ron Wyden.[4] This amendment introduced new regulation in a significantly changed online communications environment, and those twenty-six short words have entirely rewritten the history of the Internet.[5] Inserted into Title V of the Telecommunications Act (commonly known as the Communications Decency Act, or CDA) as Section 230(c)(1) (hereinafter: CDA230),[6] stating that "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."

In contrast to the U.S., the European Union chose a slightly different path of liability regulation in Article 14 of the Electronic Commerce Directive of

---

1 Seddiq, O. (2023) *Supreme Court justices aren't the 9 greatest experts on the internet, Elena Kagan said as they heard a major tech case.* [online] New York: Insider. Available from: https://www.businessinsider.com/supreme-court-google-tech-social-media-section-230-justices-internet-2023-2 [Accessed 13 June 2024].

2 *Cubby, Inc. v. Compuserve Inc.* (1991) 776 F. Supp. 135; *Stratton Oakmont, Inc. v. Prodigy Servs.* (1995) N.Y. Sup. Ct. May 24.

3 Yen, A. C. (2002) Western Frontier or Feudal Society? *Berkeley Technology Law Journal*, 17(4), p. 1210. Available from: https://doi.org/10.2139/ssrn.322522.

4 For details, see Cox, C. (2020) *The Origins and Original Intent of Section 230 of the Communications Decency Act*. [blog entry] 27 August. Richmond: Journal of Law & Technology. Available from: https://jolt.richmond.edu/2020/08/27/the-origins-and-original-intent-of-section-230-of-the-communications-decency-act [Accessed 13 June 2024].

5 Kosseff, J. (2019) *The 26 Words That Created the Internet*. New York: Cornell University Press. Available from: https://doi.org/10.7591/9781501735783.

6 Although Section 230 is part of the Telecommunications Act, it is referred to in legal and common practice as CDA230, referring to Chapter V (Communications Decency Act). Pub. L. No. 104-104 (Tit. V), 110 Stat. 133 (Feb. 8, 1996).

2000 followed and replaced in that aspect in Article 4–6 of the Digital Services Act (hereinafter: DSA) of 2022.[7] These rules "use a threefold set of definitions, the first two of which ('mere conduit' and 'caching') give service providers similar immunity from liability as under the US system."[8] Article 6 of DSA also sets up rules for a third category, the hosting providers. Under this, the hosting provider is in principle liable for the content hosted on it and is exempted from liability if:

(a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or

(b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.

Although, Tambiama Madiega noted that the European "jurisprudence on online liability today remains very fragmented",[9] it could be commented that platform providers mostly prefer to remain passive, losing the possibility of immunity from liability if they are active. In that question, the European Court of Human Rights's practice is particularly significant, in that it consciously seeks to establish more generally applicable tests that can assist parties as well as national enforcers.[10]

Based on the European-U.S. liability differences, it is worth examining where U.S. case law is heading on this question and whether there are any issues that are worthy of European attention. As the tech giants are primarily American but provide their services worldwide, European case law must pay attention to American legislation and case law in this particular matter.

In essence, the broad wording of CDA230 has enabled the development of the internet and all the exponential growth we have seen over the past two decades, as it has "enabled internet startups and their investors to populate their platforms with content from ordinary users without having to take legal responsibility for the content written by users."[11] In doing so, the legislator has made a significant contribution to the development of the internet but

---

7 Church, P. and Pehlivan, C.N. (2023) The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability. *Global Privacy Law Review*, 4(1), pp. 53-59. Available from: https://doi.org/10.54648/gplr2023005.

8 Gosztonyi, G.: *Censorship from Plato to Social Media. The Complexity of Social Media's Content Regulation and Moderation Practices*. Cham: Springer Nature Switzerland AG, p. 53. Available from: https://doi.org/10.1007/978-3-031-46529-1.

9 Madiega, T. (2020) *Reform of the EU liability regime for online intermediaries. Background on the forthcoming Digital Services Act*. Brussels: European Union, Summary.

10 *Delfi AS v Estonia* (2015). No. 64569/09, §§ 144-161, ECHR 16 June 2015; *Magyar Tartalomszolgáltatók Egyesulete and Index.hu Zrt. v Hungary* (2016). No. 22947/13, § 70, ECHR 2 February 2016; *Pihl v Sweden* (2017). No. 74742/14, § 31, ECHR 9 March 2017.

11 Reynolds, M. (2019) *The strange story of Section 230, the obscure law that created our flawed, broken internet*. [online] San Francisco: Wired. Available from:

has also addressed some of the major problems of our time. Indeed, if service providers considered that a user or a piece of content was not in their interest, they could remove it legally.[12] Even though these companies have grown to unimaginable economic power,[13] CDA230 gives them almost unlimited immunity[14] – whether they restrict or users upload inappropriate content.

Several court rulings have questioned this immunity in recent years,[15] which has led to a heated public debate about the amendment of CDA230. One example of this was then President Donald Trump's signing into law of the Fight Against Online Sex Trafficking Act (FOSTA),[16] which created an exemption to CDA230. Under the FOSTA, CDA230 cannot be invoked if the content gives rise to civil or criminal liability for conduct promoting or facilitating sex trafficking or prostitution. Still, the Act has been criticised by many for 'watering down' the basic rules of CDA230.[17]

Platforms have also set up what appear to be their own courts (such as Facebook's Oversight Board[18]) or have otherwise tried to contribute to resolving the situation themselves (such as Twitter's BlueSky initiative). In a 2020 letter from William P. Barr, the U.S. Attorney General suggested that the framework for immunity should be clarified so that platforms "cannot use

https://www.wired.co.uk/article/section-230-communications-decency-act [Accessed 13 June 2024].

[12] This is the case for the defence known only as 'good Samaritan' (CDA230(c)(2)), i.e. good faith. However, this has resulted in a paradox, as platform providers prefer to remain passive because they lose the possibility of immunity from liability if they are active. Interestingly, in the Gonzalez case before SCOTUS, Judge Ketanji Brown Jackson suggested that U.S. courts should put more emphasis on the interpretation of CDA230(c)(2), which they have failed to do so far.

[13] Birch, K. and Bronson, K. (2022) Big Tech. *Science as Culture*, 31(1), pp. 1-14. Available from: https://doi.org/10.1080/09505431.2022.2036118.

[14] For safe harbours liability, see Riordan, J. (2016) *The Liability of Internet Intermediaries*. New York: Oxford University Press, pp. 377-409. Available from: https://doi.org/10.1093/oso/9780198719779.003.0012.

[15] *Force v. Facebook, Inc* (2019) 934 F.3d 53, 64 (2d Cir. 2019), cert. denied, 140 S. Ct. 2761 (2020); *Marshall's Locksmith Serv. Inc. v. Google, LLC* (2019) 925 F.3d 1263, 1267; *Enigma Software Grp. U.S.A v. Malwarebytes, Inc.* (2019) 946 F.3d 1040, 1052 (9th Cir. 2019), cert. denied, 141 S. Ct. 13, 208 L. Ed. 2d 197 (2020).

[16] Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (the Act is often referred to as the FOSTA/SESTA Act in the United States, as an earlier version was known as the Stop Enabling Sex Traffickers Act (SESTA).

[17] Albert, K., Armbruster, E., Brundige, E., Denning, E., Kim, K., Lee, L., . . . Yang, Y. (2021) FOSTA in legal context. *Columbia Human Rights Law Review*, 52(3), pp. 1084-1158.; Ballon, i. C. (2020) *E-Commerce and Internet Law: Legal Treatise with Forms*. Los Angeles: Glasser LegalWorks.

[18] For more details, see Lendvai, G.F. (2023) "Pure Rat Country" – Reflections on Case Decision 2022-001-FB-UA of Facebook Oversight Board (Knin Cartoon Case). *Journal of Digital Technologies and Law*, 19(3); Mazur, J. and Grambličková, B. (2023) New Regulatory Force of Cyberspace: The Case of Meta's Oversight Board. *Masaryk University Journal of Law and Technology*, 17(1). Available from: https://doi.org/10.5817/MUJLT2023-1-1.

CDA230 as a shield to censor lawful speech in bad faith in ways inconsistent with their own user policies."[19] It is almost thirty years since the U.S. legislation was adopted, but the internet has changed significantly. The threshold for entry has changed, the number of users has changed, the amount of content uploaded has changed, and the technological environment has changed with it. However, the legislation remained unaltered in the previous decades. Thus, one question that needs to be answered is whether the case law must fill in the gaps in the broad wording of CDA230 or whether the politicians will clarify the rules.

On this issue, the Supreme Court of the United States of America (hereinafter: SCOTUS) took a clear position in 2023: it is not for the courts to determine the extent of the immunity provided by CDA230. This was the conclusion reached by SCOTUS in two cases that many expected to set new paths in Internet regulation and fundamentally change the liability regime that we now see as typical in the democratic part of the world. Campaigners for reconsidering CDA230 were looking forward to the SCOTUS' decision with great expectations. At the same time, tamperers feared that an over-radical decision would lead online platforms to over-removal[20] of content uploaded to them, i.e. to censorship. The significant media publicity surrounding the cases has also given rise to a new narrative that if the SCOTUS rules in favour of the plaintiffs, it could effectively "break the internet" and end freedom of expression on the internet.[21] On the latter, Google's general counsel Halimah DeLaine Prado, in a short but heated opinion piece, explicitly stresses that "if SCOTUS were to change the widely accepted application of CDA230, it would result in a digital experience – for everyone – that reflects the exact opposite of Congress' legislative intent. It would impede access to information, limit free expression, hurt the economy, and leave consumers more vulnerable to harmful online content."[22]

[19] Barr, W. P. (2020) Letter to the President of the United States. [online] Washington DC: U.S. Department of Justice. Available from: `https://www.justice.gov/file/1319346/download` [Accessed 13 June 2024].

[20] See *Delfi AS v. Estonia* (2015). No. 64569/09, § 67, ECHR 16 June 2015: "err on the side of caution to avoid possible subsequent liability".

[21] Millhiser, I. (2023) *The Supreme Court appears worried it could break the internet*. [online] New York: Vox. Available from: `https://www.vox.com/politics/2023/2/21/23608851/supreme-court-gonzalez-google-section-230-internet-twitter-facebook` [Accessed 13 June 2024].

[22] Prado, H. D. (2023) *Gonzalez v Google and the future of an open, free and safe internet*. [blog entry] 12 January. Mountain View: Google. Available from: `https://blog.google/outreach-initiatives/public-policy/gonzalez-v-google-and-the-future-of-an-open-free-and-safe-internet/` [Accessed 13 June 2024].

2. TWITTER, GOOGLE, AND THE ISIS

In the mid-2000s, the Islamic State (ISIS[23]) was seen as a real threat.[24] At the time, the Sunni jihadist organisation sought to increase its relevance by carrying out terrorist attacks beyond its borders, which also gave it significant media coverage.[25] ISIS has also carried out attacks in Europe, the most notable of which was the mass attack on the Bataclan Theatre in Paris.[26] However, smaller attacks have also resulted in numerous casualties, such as the attacks on the Paris bistro in 2015, which coincided with the Bataclan massacre, or the Istanbul nightclub[27] in 2017. The victims of these terrorist actions were not only European citizens, and the families of two victims have filed a lawsuit that also investigated the responsibility of the major social media platforms.

A woman of U.S. nationality, Nohemi Gonzalez, was killed in the Paris bistro attack, while a man of U.S.-Jordanian nationality, Nawras Alassaf, was killed in the Reina nightclub in Istanbul. The families of both victims have taken the matter to court, citing the U.S. Counterterrorism Act, and have asked a U.S. court to declare that Twitter[28] and Google[29] should be held liable for allowing content on their platforms that was linked to international terrorism.

---

[23] Islamic State of Iraq and Syria (hereinafter: ISIS). It should be noted that in the summer of 2014, ISIS renamed itself the Islamic State (IS) and declared its intention to establish a global caliphate rather than a local one. In the present study, as in the analysed SCOTUS decisions, we use the more popular ISIS acronym.

[24] Fenwick, H. (2016). Responding to the ISIS threat: extending coercive non-trial-based measures in the Counter-Terrorism and Security Act 2015. *International Review of Law Computers & Technology*, 30(3). Available from: https://doi.org/10.1080/13600869.2016.1145870.

[25] For the terrorist propaganda in social media, see Wakeford, L. and Smith, L. (2020) Islamic State's Propaganda and Social Media: Dissemination, Support, and Resilience. In: Baele, S. J., Boyd, K. A. and Coan, T. G. (eds.) *ISIS Propaganda: A Full-Spectrum Extremist Message, Causes and Consequences of Terrorism*. New York: Oxford University Press, pp. 155-187. Available from: https://doi.org/10.1093/oso/9780190932459; Shehabat, A. and Mitew, T. (2018) Black-Boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics. *Perspectives on Terrorism*, 12(1), pp. 81-99.; Lieberman, A.V. (2017) Terrorism, the Internet, and Propaganda: A Deadly Combination. *Journal of National Security Law & Policy*, 9(1), pp. 95-124.

[26] Pacelli, D., Ieracitano, F. and Rumi, C. (2019) The dimensions of fear in the storytelling of European terrorism: the case of Bataclan. In: Baygert, N., Durin, E., Le Moing-Maas, É. and Nicolas, L. (eds.) *La communication européenne, une scène de combats? Positionnements politiques et enjeux médiatiques*. Bruxelles: La Charte Professional Publishing.

[27] McKirdy, E., Yan, H. and Lee, Ian (2017) *Istanbul attack: ISIS claims nightclub shooting; killer still at large*. [online] Atlanta: CNN. Available from: `https://edition.cnn.com/2017/01/02/europe/turkey-nightclub-attack/index.html` [Accessed 13 June 2024].

[28] *Twitter, Inc. et. al. v. Taamneh et al.* (2023) 598 U.S. ___.

[29] *Gonzalez et al. v. Google, LLC* (2023) 598 U.S. ___.

In their request, the families argued that these service providers could be held liable under the secondary liability provisions[30] of the U.S. Anti-Terrorism Act.[31] Section 2333(a) of the Act states:

> *"Any national of the United States injured in his or her person, property, or business by reason of an act of international terrorism, or his or her estate, survivors, or heirs, may sue therefor in any appropriate district court of the United States and shall recover threefold the damages he or she sustains and the cost of the suit, including attorney's fees."*[32]

Another subsection of the Act provides that "liability may be asserted as to any person who aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism."[33]

The Taamneh family argued that Twitter and other companies knew that their platforms were playing an essential role in ISIS's terrorist efforts yet failed to take steps to remove illegal content from the platforms. In the other case, the Gonzalez family based their argument on the fact that Google facilitated ISIS recruitment by allowing ISIS to post videos inciting violence and recruiting potential ISIS members on YouTube[34] and by recommending ISIS videos to users through its algorithms. In addition, they argued that CDA230's immunity for platforms could not apply in cases where the platform was active, i.e. it has not acted as a sole distributor but as a publisher. Their arguments suggest this was the case here, as the platforms developed the code for the algorithm-driven targeted recommendations. In particular, the applicants' legal argument in neither case blamed the platforms for carrying out the specific attacks, but the families merely requested to establish the secondary liability based on a particular context. In both cases, the defendant's argument was similar: CDA230's immunity extends fully to the platforms, as they acted only as distributors, i.e. they had no role in producing the content. Google's lawyer, Lisa Blatt, later said, "Helping users find the proverbial needle in the haystack is a fundamental need on the Internet."[35]

---

[30] The legislation was inserted into the original text of the Justice Against Sponsors of Terrorism Act of 2015, Pub. L. 114-222 (hereinafter: JASTA).

[31] Antiterrorism Act (hereinafter: ATA), 18 U.S.C. Chapter 113B.

[32] 18 U.S.C. § 2333(a) (2015).

[33] 18 U.S.C. § 2333(d)(2) (2015).

[34] Google LLC has owned YouTube LLC since 2006 and both companies have been under the umbrella of Alphabet Inc. since 2015.

[35] Howe, A. (2023) *'Not, like, the nine greatest experts on the internet': Justices seem leery of broad ruling on Section 230*. [blog entry] 21 February. Bethesda: SCOTUSblog. Available from: `https://www.scotusblog.com/2023/02/not-like-the-nine-greatest-`

As a result of the proceedings in the lower courts,[36] the two cases – which are legally similar in a fundamental sense – raised different issues by the time they reached SCOTUS. In the Gonzalez case, the Court had to decide whether CDA230 covered algorithm-driven recommender systems and whether the Ninth Circuit Court of Appeals (USCNC) was correct in holding that the algorithms of the major online platforms operate in a neutral manner, i.e., they recommend content to users based solely on search history and interests.[37] In the Taamneh case, however, SCOTUS had to rule on liability under the ATA and JASTA. The arguments before SCOTUS demonstrated how the legal issues in the two cases are inseparable, and the arguments on both sides of the cases have become confusing. SCOTUS also had to take a position on the so-called chilling effect,[38] as large online platforms are known to receive more and more requests from authoritarian or quasi-authoritarian governments to remove material posted on them.[39]

3. THE LEGAL PROCEDURE

SCOTUS started hearing the two cases together in October 2022, and the decision was handed down on May 18, 2023. The decision was noted by Justice Clarence Thomas, who pointed out that the amount of content being shared and uploaded on the giant platforms was staggering. YouTube, Facebook and Twitter were marked as examples, underlining that the monthly active users on these platforms could reach billions and that hundreds of thousands of pieces of content were uploaded to these platforms every minute.[40] Judge Thomas also indicated that the content created by members and supporters of ISIS who glorified the terrorists who had committed the attacks was harmful and damaging.[41] Concerning the ATA,

---

experts-on-the-internet-justices-seem-leery-of-broad-ruling-on-section-230/ [Accessed 13 June 2024].

[36] *Gonzalez et al. v. Google, LLC* (2021) 18-16700; *Taamneh et al. v. Twitter, Inc. et al.* (2021) 18-17192.

[37] This argument was rejected by Judge Gould in his dissenting opinion because "where the website (1) knowingly amplifies a message designed to recruit individuals for a criminal purpose, and (2) the dissemination of that message materially contributes to a centralized cause giving rise to a probability of grave harm, then the tools can no longer be considered neutral." Judge Gould did not rule out the possibility that an algorithm could be neutral (citing *Carafano v. Metrosplash.com, Inc.* (2003) 339 F.3d 1119, 1123, as an example), but in the present case he found this reasoning unavailing (*Gonzalez et al. v. Google, LLC* (2021) 18-16700, p. 100).

[38] Pech, L. (2021) *The Concept of Chilling Effect. Its untapped potential to better protect democracy, the rule of law, and fundamental rights in the EU*. Brussels: Open Society European Policy Institute.

[39] Jurecic, Q., Rozenshtein, A. Z. and Wittes, B. (2023) *Have the Justices Gotten Cold Feet About 'Breaking the Internet'?* [blog entry] 24 February. Washington DC: Lawfare. Available from: https://www.lawfaremedia.org/article/have-justices-gotten-cold-feet-about-breaking-internet [Accessed 13 June 2024].

[40] *Twitter, Inc. et. al. v. Taamneh et al.* (2023) 598 U.S. ___, pp. 3-4.

[41] *Op. cit.*, p. 5.

SCOTUS also interpreted and ruled on Section 2333(a), stating that the critical issue in the case was to determine whether the platforms, as defendants, knowingly provided substantial assistance to the commission of the terrorist action or, more simply put, whether the distribution of terrorist content could constitute aiding and abetting.[42]

The SCOTUS examined what was meant by aiding and abetting and what Twitter did to aid and abet the terrorists.[43] Here, the SCOTUS recalled, with particular reference to JASTA, the Halberstam case – a leading case on aiding, abetting, and liability for conspiracy.[44] With that case reference, SCOTUS proposed three crucial criteria for establishing aiding and abetting in the Taamneh case. First, the aiding and abetting party must assist in an unlawful activity that causes harm. Second, the party must know that its involvement is part of the illegal activity. Thirdly, the assistance must be substantial in addition to being known. However, Judge Thomas pointed to the fact that assistance is not a "limitless concept" and that the applicability of the Halberstam case was very difficult because of the substantial differences between the facts, thus pointing out that the USCNC had driven an analogy too close between the Taamneh case and the Halberstam case. As a sub-conclusion could be drawn, there were no helpful analogies for the judges to decide in these cases.

The SCOTUS paid even more attention to determining what, if anything, was the activity that Twitter aided and abetted as a potential accomplice. A key segment of Justice Thomas's opinion explained that the plaintiffs' and defendants' arguments were both based on flawed premises. The plaintiffs overly adhered to the Halberstam case and failed to consider that the aiding and abetting, in that case, was established because of being systematic, while the defendants overstated the nexus required by Section 2333(d)(2) between the alleged aiding and abetting and the tort since the accomplice need not have detailed knowledge of the terrorist's plan.[45] Indeed, the correct interpretation, and thus the correct reasoning, would have been for the plaintiffs to prove that Twitter provided such knowing and substantial assistance to ISIS that it could be construed as culpable participation in the Istanbul attack, and the defendant, by implication, the opposite.[46]

According to SCOTUS, the plaintiffs failed to prove that Twitter knowingly and substantially aided and abetted the terrorist attack. Concerning the nature of the content and the algorithms, the opinion

[42] *Op. cit.,* p. 8.
[43] *Ibid*.
[44] *Halberstam v. Welch* (1983) 705 F. 2d 472.
[45] *Twitter, Inc. et. al. v. Taamneh et al.* (2023) 598 U.S. ___, p. 19.
[46] *Op. cit.,* p. 21.

highlighted that although ISIS activists and sympathisers were indeed present on the social media platform, and the algorithmic recommendation system did certainly offer ISIS-related content to users whom the algorithm assumed would be interested in such content, the issue of guilt was not proven.[47] This was upheld by the SCOTUS, although, overall, the fact that the platforms, in most cases, did not exercise a (pro)active attitude to prevent the algorithm from filtering out the recommendation of terrorist content was not in dispute.

Judge Thomas drew a particularly significant analogy in this respect between platforms and earlier technologies, namely mobile phones. For example, is a telephone company liable for having brokered several transactions involving illegal substances via mobile phone?[48] The SCOTUS answered the question in the negative, even though there was no doubt that the telephone call facilitated the transaction. The importance of this example, however, is that the plaintiffs ultimately argue that the algorithms' recommendations constitute "active" assistance, which was not the case, as the plaintiffs have failed to prove that Twitter's algorithms intentionally, knowingly and materially recommended ISIS content knowing that it would or could lead to the Istanbul attack. According to SCOTUS, the algorithms are neutrals, and there was no specific outreach connected with the attack or even ISIS. Concerning platform liability, SCOTUS also indicated that the "plaintiffs identify no duty that would require defendants or other communication-providing services to terminate customers after discovering that the customers were using the service for illicit ends".[49] Moreover, even if such an obligation could be identified, proving that the defendant platforms knowingly failed to act with intent to assist in recommending ISIS content to users would again raise concerns.

The SCOTUS also adopted the USCNC's proposal for the Halberstam framework, now applying it correctly. It pointed out that the USCNC erred in its decision to separate the concepts of knowing and substantial, as the awareness of the tech giants that ISIS content was present on their platforms can only be interpreted as general awareness. It cannot be construed as knowledge of and assistance with a specific, individual act of terrorism. The SCOTUS also underlined that the USCNC had misinterpreted the algorithms as technical means, as algorithmic referral systems were not only exclusively

[47] *Op. cit.*, p. 22.
[48] Cf. *Doe v. GTE Corp* (2003) 347 F.3d (CA7).
[49] *Twitter, Inc. et. al. v. Taamneh et al.* (2023) 598 U.S. ___, p. 25.

available to ISIS militants but to the whole general public.[50] In essence, the plaintiffs have alleged that the defendants generally provided available virtual platforms that ISIS used and that the defendants did not stop ISIS despite knowing that it was using those platforms.[51] This allegation was insufficient to establish a credible correlation between the Reina attack and the recommendation systems. The SCOTUS also agreed with the USCNC, which found no credible evidence that Google intentionally supported and aided ISIS by operating its revenue-sharing system. Overall, the SCOTUS in the case found no connection between the defendants and the Reina attack. In light of the above, the SCOTUS reversed the USCNC's judgment.

This detailed description of the Taamneh case also helps to understand the highly terse (only three pages) per curiam opinion of the SCOTUS in the Gonzalez case, given that the decision was essentially based entirely on the Taamneh case. SCOTUS claimed that in the absence of aiding and abetting, the ruling would have been limited to the sole issue of whether Google was responsible for the terrorist actions committed by ISIS through revenue sharing. At the oral hearing on 21 February 2023, the plaintiffs requested to amend their claims. SCOTUS noted in response that it was not its role to grant such requests; however, the SCOTUS judges found and conceded that the plaintiffs' arguments were not supported by either the USCNC or the above Taamneh decision. Consequently, the SCOTUS did not consider the applicability or even possible modification of CDA230 but vacated the judgment and remanded the case to the USCNC to reconsider the plaintiffs' complaint in light of the Taamneh judgment.[52]

4. CONCLUSION

The international legal press and legal blogs were full of such questions after the ruling: Has SCOTUS crashed the internet? Has an all-overriding, game-changing precedent been set? Can algorithms be used to support acts of terrorism? The answer to all three questions was negative. "As much as the SCOTUS judges disliked the fact that social media platforms encourage users to watch ISIS videos, none of them seemed open to holding Google accountable for trying to create the best search engine possible."[53]

[50] Cf.: „Rather, defendants' relationship with ISIS and its supporters appears to have been the same as their relationship with their billion-plus other users: arm's length, passive, and largely indifferent." *Twitter, Inc. et. al. v. Taamneh et al.* (2023) 598 U.S. ___, p. 24.

[51] *Op. cit.*, pp. 28-29.

[52] *Gonzalez et al. v. Google, LLC* (2023) 598 U.S. ___, p. 3.

[53] Jurecic, Q., Rozenshtein, A. Z. and Wittes, B. (2023) *Have the Justices Gotten Cold Feet About 'Breaking the Internet'?* [blog entry] 24 February. Washington DC: Lawfare. Available from: `https://www.lawfaremedia.org/article/have-justices-gotten-cold-feet-about-breaking-internet` [Accessed 13 June 2024].

SCOTUS' reasoning showed that if the same algorithm that was accepted to recommend cooking videos to people based on their search history and interests recommends terrorist content to other people based on the same search history and interests, it was difficult to hold it accountable.

However, regarding CDA230 and the algorithm relationship, the decisions were undoubtedly prominent as SCOTUS evaluated algorithmic recommendation systems as a method, a neutral tool used by platforms[54] rather than a deliberate activity by the platforms. In this respect, the SCOTUS's conservative and nuanced approach to the relationship between algorithms and CDA230 is to be welcomed – regulating algorithms in a comprehensive, separate regulation[55] is more welcome rather than reforming CDA230 just because platforms use algorithms.

The main question is whether these two decisions would lead to the end of the revision of CDA230, i.e., have the Gonzalez and Taamneh cases closed the "twenty-six words question"? The answer is again negative. It is worth highlighting Texas House Bill 20,[56] which aimed to prevent users from being banned or denied access to platforms because of their views and opinions.[57] Although the law came into force in September 2021, the plaintiff in NetChoice v. Paxton asked that the enforcement be denied.[58] The case is currently before the SCOTUS, as the Fifth Circuit Court of Appeals overturned the federal decision by a 2-1 vote, allowing the Texas law to be applied and enforced. The SCOTUS ruling will undoubtedly be an essential step in the evolution of CDA230, so the end is not close.

Article-19 has hailed the Taamneh and Gonzalez decisions as a significant victory for freedom of expression online,[59] as "the Internet has now become one of the principal means by which individuals exercise their right to

[54] Kenneth, T. and Rubinstein, I. (2023) Gonzalez v. Google: The Case for Protecting "Targeted Recommendations". *Duke Law Journal Online*, 72, p. 197. Available from: https://doi.org/10.2139/ssrn.4337584.

[55] In October 2023, Joe Biden signed an Executive Order to address the problems caused by artificial intelligence. Lendvai, G.F. and Gosztonyi, G. (2024) Deepfake y desinformación. ¿Qué puede hacer el derecho frente a las noticias falsas creadas por deepfake? [in press] Submitted to: *IDP. Revista de Internet, Derecho y Política*.

[56] Texas House Bill 20 (HB20), An Act Relating to censorship of or certain other interference with digital expression, including expression on social media platforms or through electronic mail messages.

[57] Robertson, A. (2021) Texas passes law that bans kicking people off social media based on 'viewpoint'. [online] New York: The Verge. Available from: `https://www.theverge.com/2021/9/9/22661626/texas-social-media-law-hb-20-signed-greg-abbott` [Accessed 13 June 2024].

[58] *NetChoice, LLC v. Paxton* (2022) 49 F.4th 439.

[59] ARTICLE 19 (2023) *United States: clear victory for free speech in the Supreme Court decisions*. [online] London: ARTICLE 19. Available from: `https://www.article19.org/resources/united-states-clear-victory-for-free-speech-in-the-supreme-court-decisions/` [Accessed 13 June 2024].

freedom to receive and impart information and ideas",[60] and any restrictions would jeopardise this. While it may seem that the SCOTUS judges were trying to deflect by stating that their ability to consider the complex technical issues involved was limited because they were not Internet experts, they took the correct legal position. They have decided that the legislators cannot use the judicial system as a proxy to solve the problems instead of them. The SCOTUS decision points to the fact that the fate of CDA230 and the "breaking or regulating giant platforms"[61] is in the hands of nothing but legislators.

LIST OF REFERENCES

[1] Albert, K., Armbruster, E., Brundige, E., Denning, E., Kim, K., Lee, L., Yang, Y. (2020) FOSTA in Legal Context. Columbia Human Rights Law Review, 2021, Vol. 52, No. 3.

[2] Allow States and Victims to Fight Online Sex Trafficking Act of 2017

[3] Antiterrorism Act, 18 U.S.C. Chapter 113B

[4] ARTICLE 19 (2023) *United States: clear victory for free speech in the Supreme Court decisions*. [online] London: ARTICLE 19. Available from: https://www.article19.org/resources/united-states-clear-victory-for-free-speech-in-the-supreme-court-decisions/ [Accessed 13 June 2024].

[5] Ballon, i. C. (2020) *E-Commerce and Internet Law: Legal Treatise with Forms*. Los Angeles: Glasser LegalWorks

[6] Barr, W. P. (2020) Letter to the President of the United States. [online] Washington DC: U.S. Department of Justice. Available from: https://www.justice.gov/file/1319346/download [Accessed 13 June 2024]

[7] Birch, K. and Bronson, K. (2022) Big Tech. *Science as Culture*, 31(1). Available from: https://doi.org/10.1080/09505431.2022.2036118.

[8] *Carafano v. Metrosplash.com, Inc.* (2003) 339 F.3d 1119, 1123.

[9] *Cengiz and Others v. Turkey* (2015). Nos 48226/10 and 14027/11, § 49, ECHR 1 December 2015.

[10] Church, P. and Pehlivan, C.N. (2023) The Digital Services Act (DSA): A New Era for Online Harms and Intermediary

[60] *Cengiz and Others v. Turkey* (2015). Nos 48226/10 and 14027/11, § 49, ECHR 1 December 2015.

[61] Jurecic, Q., Rozenshtein, A. Z. and Wittes, B. (2023) *Have the Justices Gotten Cold Feet About 'Breaking the Internet'?* [blog entry] 24 February. Washington DC: Lawfare. Available from: https://www.lawfaremedia.org/article/have-justices-gotten-cold-feet-about-breaking-internet [Accessed 13 June 2024].

Liability. *Global Privacy Law Review*, 4(1). Available from: https://doi.org/10.54648/gplr2023005.

[11] Communications Decency Act Pub. L. No. 104-104 (Tit. V), 110 Stat. 133 (Feb. 8, 1996)

[12] Cox, C. (2020) *The Origins and Original Intent of Section 230 of the Communications Decency Act*. [blog entry] 27 August. Richmond: Journal of Law & Technology. Available from: `https://jolt.richmond.edu/2020/08/27/the-origins-and-original-intent-of-section-230-of-the-communications-decency-act` [Accessed 13 June 2024].

[13] *Cubby, Inc. v. Compuserve Inc.* (1991) 776 F. Supp. 135.

[14] *Delfi AS v. Estonia* (2015). No. 64569/09, ECHR 16 June 2015.

[15] *Doe v. GTE Corp* (2003) 347 F.3d (CA7).

[16] *Enigma Software Grp. U.S.A v. Malwarebytes, Inc.* (2019) 946 F.3d 1040, 1052 (9th Cir. 2019), cert. denied, 141 S. Ct. 13, 208 L. Ed. 2d 197 (2020).

[17] Fenwick, H. (2016). Responding to the ISIS threat: extending coercive non-trial-based measures in the Counter-Terrorism and Security Act 2015. *International Review of Law Computers & Technology*, 30(3). Available from: https://doi.org/10.1080/13600869.2016.1145870.

[18] *Force v. Facebook, Inc* (2019) 934 F.3d 53, 64 (2d Cir. 2019), cert. denied, 140 S. Ct. 2761 (2020).

[19] *Gonzalez et al. v. Google, LLC* (2021) 18-16700.

[20] *Gonzalez et al. v. Google, LLC* (2023) 598 U.S. ___.

[21] Gosztonyi, G.: *Censorship from Plato to Social Media. The Complexity of Social Media's Content Regulation and Moderation Practices*. Cham: Springer Nature Switzerland AG. Available from: https://doi.org/10.1007/978-3-031-46529-1.

[22] *Halberstam v. Welch* (1983) 705 F. 2d 472.

[23] Howe, A. (2023) *'Not, like, the nine greatest experts on the internet': Justices seem leery of broad ruling on Section 230*. [blog entry] 21 February. Bethesda: SCOTUSblog. Available from: `https://www.scotusblog.com/2023/02/not-like-the-nine-greatest-experts-on-the-internet-justices-seem-leery-of-broad-ruling-on-section-230/` [Accessed 13 June 2024].

[24] Jurecic, Q., Rozenshtein, A. Z. and Wittes, B. (2023) *Have the Justices Gotten Cold Feet About 'Breaking the Internet'?* [blog entry]

24 February. Washington DC: Lawfare. Available from: https://www.lawfaremedia.org/article/have-justices-gotten-cold-feet-about-breaking-internet [Accessed 13 June 2024].

[25] Justice Against Sponsors of Terrorism Act, Pub. L. 114-222

[26] Kenneth, T. and Rubinstein, I. (2023) Gonzalez v. Google: The Case for Protecting "Targeted Recommendations". *Duke Law Journal Online*, 72. Available from: https://doi.org/10.2139/ssrn.4337584.

[27] Kosseff, J. (2019) *The 26 Words That Created the Internet*. New York: Cornell University Press. Available from: https://doi.org/10.7591/9781501735783.

[28] Lendvai, G.F. (2023) "Pure Rat Country" – Reflections on Case Decision 2022-001-FB-UA of Facebook Oversight Board (Knin Cartoon Case). *Journal of Digital Technologies and Law*, 19(3).

[29] Lendvai, G.F. and Gosztonyi, G. (2024) Deepfake y desinformación. ¿Qué puede hacer el derecho frente a las noticias falsas creadas por deepfake? [in press] Submitted to: *IDP. Revista de Internet, Derecho y Política*.

[30] Lieberman, A.V. (2017) Terrorism, the Internet, and Propaganda: A Deadly Combination. *Journal of National Security Law & Policy*, 9(1).

[31] *Magyar Tartalomszolgáltatók Egyesulete and Index.hu Zrt. v Hungary* (2016). No. 22947/13, ECHR 2 February 2016

[32] *Marshall's Locksmith Serv. Inc. v. Google, LLC* (2019) 925 F.3d 1263, 1267.

[33] Mazur, J. and Gramblička, B. (2023) New Regulatory Force of Cyberspace: The Case of Meta's Oversight Board. *Masaryk University Journal of Law and Technology*, 17(1). Available from: https://doi.org/10.5817/MUJLT2023-1-1

[34] McKirdy, E., Yan, H. and Lee, Ian (2017) *Istanbul attack: ISIS claims nightclub shooting; killer still at large*. [online] Atlanta: CNN. Available from: https://edition.cnn.com/2017/01/02/europe/turkey-nightclub-attack/index.html [Accessed 13 June 2024].

[35] Millhiser, I. (2023) *The Supreme Court appears worried it could break the internet*. [online] New York: Vox. Available from: https://www.vox.com/politics/2023/2/21/23608851/supreme-court-gonzalez-google-section-230-internet-twitter-facebook [Accessed 13 June 2024].

[36] *NetChoice, LLC v. Paxton* (2022) 49 F.4th 439.

[37] Pacelli, D., Ieracitano, F. and Rumi, C. (2019) The dimensions of fear in the storytelling of European terrorism: the case of Bataclan. In: Baygert, N., Durin, E., Le Moing-Maas, É. and Nicolas, L. (eds.) *La communication européenne, une scène de combats? Positionnements politiques et enjeux médiatiques*. Bruxelles: La Charte Professional Publishing.

[38] Pech, L. (2021) *The Concept of Chilling Effect. Its untapped potential to better protect democracy, the rule of law, and fundamental rights in the EU*. Brussels: Open Society European Policy Institute.

[39] *Pihl v Sweden* (2017). No. 74742/14, ECHR 9 March 2017.

[40] Prado, H. D. (2023) *Gonzalez v Google and the future of an open, free and safe internet*. [blog entry] 12 January. Mountain View: Google. Available from: https://blog.google/outreach-initiatives/public-policy/gonzalez-v-google-and-the-future-of-an-open-free-and-safe-internet/ [Accessed 13 June 2024].

[41] Reynolds, M. (2019) *The strange story of Section 230, the obscure law that created our flawed, broken internet*. [online] San Francisco: Wired. Available from: https://www.wired.co.uk/article/section-230-communications-decency-act [Accessed 13 June 2024].

[42] Riordan, J. (2016) *The Liability of Internet Intermediaries*. New York: Oxford University Press. Available from: https://doi.org/10.1093/oso/9780198719779.003.0012.

[43] Robertson, A. (2021) Texas passes law that bans kicking people off social media based on 'viewpoint'. [online] New York: The Verge. Available from: https://www.theverge.com/2021/9/9/22661626/texas-social-media-law-hb-20-signed-greg-abbott [Accessed 13 June 2024].

[44] Seddiq, O. (2023) *Supreme Court justices aren't the 9 greatest experts on the internet, Elena Kagan said as they heard a major tech case*. [online] New York: Insider. Available from: https://www.businessinsider.com/supreme-court-google-tech-social-media-section-230-justices-internet-2023-2 [Accessed 13 June 2024].

[45] Shehabat, A. and Mitew, T. (2018) Black-Boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics. *Perspectives on Terrorism*, 12(1), pp. 81-99.; Lieberman, A.V. (2017) Terrorism, the Internet, and Propaganda: A Deadly Combination. *Journal of National Security Law & Policy*, 9(1).

[46] *Stratton Oakmont, Inc. v. Prodigy Servs.* (1995) N.Y. Sup. Ct. May 24.

[47] *Taamneh et al. v. Twitter, Inc. et al.* (2021) 18-17192.

[48] Texas House Bill 20 (HB20), An Act Relating to censorship of or certain other interference with digital expression, including expression on social media platforms or through electronic mail messages.

[49] *Twitter, Inc. et. al. v. Taamneh et al.* (2023) 598 U.S. ___.

[50] Wakeford, L. and Smith, L. (2020) Islamic State's Propaganda and Social Media: Dissemination, Support, and Resilience. In: Baele, S. J., Boyd, K. A. and Coan, T. G. (eds.) *ISIS Propaganda: A Full-Spectrum Extremist Message, Causes and Consequences of Terrorism*. New York: Oxford University Press. Available from: https://doi.org/10.1093/oso/9780190932459.

[51] Yen, A. C. (2002) Western Frontier or Feudal Society? *Berkeley Technology Law Journal*, 17(4). Available from: https://doi.org/10.2139/ssrn.322522.