World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

Check for updates

Rethinking Section 230: Toward alternative strategies for protecting user privacy in the age of surveillance capitalism

Amaka Peace Onebunne *

Department of Communication, Northern Illinois University.

World Journal of Advanced Research and Reviews, 2024, 24(03), 3339-3345

Publication history: Received on 02 November 2024; revised on 28 December 2024; accepted on 30 December 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.24.3.3445

Abstract

This paper critically examines the intersection of Section 230 of the Communications Decency Act (CDA) and surveillance capitalism, focusing on the inadequacies of the current legal framework in protecting users' privacy in the age of automation. Using *Google v. Gonzalez* as a case study, it discusses the implications of Section 230 on privacy rights and the ethical frictions brought about by algorithmic content recommendation systems. Systems, while designed for better user experience, also exploit user data compromising privacy and exposing users to manipulation, biased framing, and increasingly polarized digital environments. Thus, this paper proposes alternative strategies, including regulatory reforms, the adoption of privacy-enhancing technologies, and the development of ethical models for platform governance. These measures aim to realign legal protections with the evolving realities of the digital economy.

Keywords: Surveillance Capitalism; User Privacy; Algorithmic Content Recommendation; Communication Decency Act (CDA); Platform Governance

1. Introduction

Advancement of digital technologies has raised salient concerns about privacy and data exploitation in the age of surveillance capitalism. While Section 230 of the Communications Decency Act (CDA) was initially pivotal in shaping the modern internet by protecting platforms from liability for user-generated content, it has not kept pace with the advancements of the digital economy. Originally designed in 1996 to promote free speech and innovation, Section 230 now faces scrutiny in an era where algorithms and data-driven technologies dominate online interactions.

The rise of algorithmic content recommendation systems, such as those employed by YouTube and other platforms, shows one of the many challenges of modern internet. These systems, powered by user data, do more than just host content—they shape user experiences, influence engagement, and often amplify harmful or polarizing content without users' explicit knowledge or consent. This shift from passive hosting to active content curation highlights a critical gap in Section 230's ability to protect individuals from the harms of data exploitation and algorithmic manipulation.

A key example of these challenges is the case of *Gonzalez v. Google* (2023), which stresses the urgent need for reform. In this case, Google's algorithmic recommendation system on YouTube was alleged of playing a role in radicalizing individuals by promoting harmful content, raising important questions about the responsibility platforms should bear for the content they amplify. This case, among others, reveals the growing disconnect between laws like Section 230 and the complex reality of today's digital platforms.

Thus, this paper critically examines the inadequacies of Section 230 in addressing the privacy risks posed by surveillance capitalism. Drawing on the *Gonzalez v. Google* case, this paper argues that Section 230 requires reform to

* Corresponding author: Amaka Peace Onebunne, ORCiD ID: https://orcid.org/0009-0000-3029-5987

account for the operational advancements of digital platforms and proposes alternative strategies that align legal protections with the evolving realities of the modern internet.

2. Section 230 of the CDA

Section 230 of the CDA, as often referred to as "the twenty-six words that created the internet," by Kosseff (2019) was enacted as a part of the broader Telecommunications Act of 1996. In the landmark case of Stratton Oakmont, Inc. v. Prodigy Services Co., (1995), Prodigy was sued for defamation over user-generated content posted on its bulletin board system. The court held Prodigy liable as a publisher of the defamatory content because it actively moderated and edited user posts, which led the court to conclude that Prodigy exercised editorial control over the content. The ruling in *Stratton Oakmont* created a chilling effect on online platforms, discouraging them from moderating content for fear of being held liable as publishers. It can be argued that while there was not a single case that directly led to the creation of Section 230, the legal discourses surrounding online liability, particularly highlighted by cases like Stratton Oakmont v. Prodigy, played a significant role in prompting Congress to enact Section 230 to provide clarity and protection for online platforms. To reaffirm, Section 230 of the CDA has been instrumental in encouraging innovation and enabling free expression online over the past 28 years. This is true, especially for legal scholars like Kosseff (2019), who have praised Section 230 for its role in enabling the growth of the internet, arguing that it has allowed platforms to flourish by removing the fear of crippling legal liability.

But the internet has dramatically evolved since the enactment of Section 230 in 1996, and with this evolution comes the need to reassess its application. One significant shift lies in the rise of autonomous agents, like algorithms, which operate within the spaces sponsored by online platforms. These algorithms are powered by vast amounts of user data and play a key role in shaping the content users encounter, often without their explicit knowledge or consent.

3. Surveillance Capitalism

One key figure in the discussion on surveillance capitalism is Shoshana Zuboff (2019). She conveyed the idea of surveillance capitalism as t new form of capitalism that revolves around the commodification of personal data. In this economic model, companies employ extensive tracking mechanisms, using tools like cookies, tracking pixels, and other digital fingerprinting technologies. The goal is to exploit user behavior, preferences, and interactions to maximize profit, often through highly targeted advertising and personalized recommendations.

Digital technologies like the mobile phones and digital platforms have long created new categories of social relations that facilitated connectivity and access to information across geographical borders bringing out the concept of present absence according to Fortunati (2002). With users constantly being online, this translates to more digital interactions, like clicks, likes, scrolling, personal profiles, etc., and massive digital footprints left behind. These technologies, having okayed companies to track their user' online interactions, preferences, and behaviors laid the groundwork for the data-driven economy. Zuboff (2019) made the argument that these practices are ongoing due to a hyper-capitalist framework that is rooted in neo-liberal economics, which prioritizes deregulation, market competition, and maximization of shareholder value. Here, companies are incentivized to extract value from every aspect of human experience, including the intimate details of individuals' lives captured through data surveillance. In this economic model, personal data is thus treated as a tradable commodity, bought, and sold in increasingly opaque and unregulated markets. Companies use this data for a number of things including fueling targeted advertising, personalizing recommendations, and algorithmic decision-making, all aimed at maximizing profits and market dominance.

The idea of data commodification has also been discussed widely by different authors. On the self, Chisnall (2020) talked about this with 'digital slavery' as a term to convey the concept of data extraction as a practice of 'owing' rooted in the historical slavery, and dual alienation of the self. One way to this alienation is that this practice portrays the idea of being subjected to a state of ownership, akin to property, by an Other. While the other way is diminishing the capacity of users to exercise control over their own existence. The self here is a digital representation of the physical self, a dossier of sorts, which further adds to the understanding of the self and autonomy. Other key authors on the appropriation of data are Couldry and Mejias (2019) who used the term 'data colonialism' as a concept that represents a new phase of capitalism, wherein the commodification of user data is normalized. As in colonialism, they argue that user data is similarly expropriated and exploited for profit by a powerful Other who believes they know how best to use the data more than the original owners. This not only creates a new social order of continuous surveillance and monitoring that extends capitalism but also erodes user privacy, autonomy, and overall societal well-being.

The legal and ethical consequences of surveillance capitalism come into sharp focus in cases like *Gonzalez v. Google*. Platforms like YouTube, driven by surveillance capitalist models, use algorithmic recommendation systems to maximize engagement and profit. These systems rely heavily on user data, shaping what content users see, often with little transparency about how decisions are made. The case highlights the tension between surveillance capitalism's need for data-driven engagement and the lack of accountability for the harmful content these algorithms can amplify. This raises important legal questions about the role of Section 230 in shielding platforms from liability for the consequences of these algorithmic decisions. It is true that Section 230 was designed to protect platforms from being treated as publishers, it was not written with algorithmic amplification in mind.

4. Privacy

Privacy as a concept has legal, philosophical, cultural, and social dimensions which cannot be discussed in depth here. One of the most prominent voices in privacy studies, Solove (2009), points out that due to the varied dimensions of privacy, it is usually hard to get a definitive ontology of privacy issues as they are often contextual and applied or interpreted on a case-by-case basis. Solove developed a taxonomy of privacy that categorizes privacy-related concerns into four main areas: information collection, information processing, information dissemination, and invasion. This categorization provides a framework for understanding the various ways privacy can be compromised in data-driven era. However, this framework is not entirely impartial and may involve subjective judgments, according to Solove (2009). It also helps researchers, policymakers, and users to identify and address specific threats to privacy and develop appropriate protective measures.

The information collection category focuses on the gathering of personal information. Information collection strategies like surveillance have the potential to induce self-censorship and restraint, making it a means of social control due to its inhibiting effects. This alludes to the position of Chisnall (2020) on how this kind of 'gaze' alienates the self. Information collection poses risks to privacy as it involves the accumulation of potentially sensitive data with or without individuals' knowledge or consent.

Consent usually implies that individuals are aware of and agree to the collection and use of their data, potentially diminishing the perception of that information as private. Yet, this perspective overlooks several critical factors. First, the conditions under which consent is obtained are often problematic. Many users may not fully understand the extent of the data collection, the ways their data will be used, or the potential risks involved. In many cases, consent is obtained through lengthy, complex terms and conditions that few read thoroughly (Obar & Oeldorf-Hirsch, 2020). Also, sometimes, giving consent does not necessarily reflect a voluntary and informed decision. It could be driven by necessity—for instance, when using essential services online or using popular digital platforms— opting out may not be a viable option. This form of *coerced* consent cripples the notion that the individual has freely chosen to share their private information.

The category of information processing looks at concerns related to how data is stored, analyzed, and used. Examples include data aggregation, profiling, etc. Given how social media platforms function, this can lead to privacy violations when data is used in ways that individuals did not anticipate or consent to, such as targeted advertising or discriminatory profiling. The information dissemination category focuses on the distribution and sharing of personal information. It includes concerns about who has access to data, how it is shared, and the potential consequences of its dissemination. Examples include data breaches, unauthorized disclosures, and data sharing among third parties. The invasion category involves direct intrusions into individuals' private spaces or activities. These spaces may be physical or virtual trespassing, surveillance, location tracking, and monitoring, etc.

Again, as opined by Solove, this is not definite, because it will mean giving an overly simplistic lens to a topic as complex as privacy. Solove's Taxonomy highlights that these autonomous agents stand to benefit from this large amount of user information already amassed by online platforms in the information collection stage. They analyze user behavior, preferences, and interactions to tailor content recommendations, personalize advertisements, and even make decisions impacting users' lives. Unlike human actors, these algorithms are much faster in speed, scale, and opacity, thus raising concerns about accountability, transparency, and the protection of user rights. Scholars like Kelly (2019) have shed light on how Instagram's algorithms wield significant influence over user decisions, often in ways that extend far beyond individual autonomy through algorithms that are designed to prioritize content that elicits strong emotional reactions and/or captures users' attention, often regardless of its accuracy. This means, there is a need to revisit Section 230.

5. Gonzalez v. Google 2023

In 2015, Nohemi Gonzalez, a U.S. citizen, was tragically killed in the Paris terrorist attacks carried out by ISIS. Following this, her family filed a lawsuit against Google under 18 U.S.C. §§2333(a) and (d)(2), claiming that YouTube, a platform owned by Google, played a role in radicalizing individuals responsible for the attack. The lawsuit centered on the argument that YouTube's algorithmic recommendation system, which promotes content based on user behavior, was not just a passive tool but actively contributed to the dissemination of ISIS propaganda. By promoting these videos, the family argued that Google became complicit in amplifying harmful content, moving beyond the protections typically offered under Section 230 of the Communications Decency Act (CDA).

The family further alleged that YouTube's revenue-sharing system, which monetizes content through advertisements, enabled ISIS to benefit financially from its videos. As a result, they claimed that Google should be held both directly and secondarily liable for aiding in the radicalization process that led to the Paris attacks, challenging the immunity typically provided by Section 230.

Google, in response, maintained that Section 230 of the CDA protected platforms like YouTube from lawsuits related to user-generated content. They argued that this legal protection is essential for maintaining open internet services and facilitating the moderation of content without exposing platforms to overwhelming legal risks. Google emphasized that Section 230 allows them to continue operating their platforms freely, without fear of liability for content created by others.

Initially, the District Court dismissed most of the claims based on Section 230, which shields platforms from liability for third-party content. However, the court allowed claims related to 'direct and secondary liability' to proceed. The case was remanded for further consideration following the decision in *Twitter, Inc. v. Taamneh*. In that case, Taamneh was unable to establish a claim for 'aiding and abetting' under §2333(d)(2), leading the Ninth Circuit to similarly rule in the *Gonzalez* case. The court found that Gonzalez's family had failed to establish a valid legal claim of aiding and abetting terrorism, concluding that there was no evidence of an agreement between Google and ISIS to support claims of conspiracy liability. Furthermore, the plaintiffs could not demonstrate that Google's actions were intended to intimidate civilians or influence government actions, which is necessary to establish direct liability under §2333(a).

6. Discussion

The *Gonzalez v. Google* case brings to the fore many key issues at the crossroad of Section 230, algorithmic content recommendation systems, and platform accountability, particularly as they relate to privacy, user safety, and the amplification of harmful content. Central to the case is the question of whether the broad immunity offered under Section 230 of the Communications Decency Act is sufficient in an era where digital platforms are no longer passive hosts of content but active curators and amplifiers of information through advanced algorithms.

6.1. Algorithmic Amplification and Platform Responsibility

One of the arguments raised in the case above was that YouTube's algorithmic recommendation system played an active role in disseminating ISIS propaganda by suggesting related content to users based on their viewing history. This raises key questions about the nature of algorithmic recommendation systems and the degree of responsibility platforms should bear for the content they amplify. Traditionally, Section 230 has shielded platforms from liability for user-generated content, but the *Gonzalez* family contended that by recommending specific content, YouTube went beyond passive hosting and became an active participant in the distribution of harmful material.

This argument touches on a critical gap in Section 230's original scope. The law was written in 1996, long before the advent of algorithmic recommendation systems that shape what users see and consume. This has given platforms a unique ability to influence user behavior, making the question of responsibility for harmful content all the more critical. As platforms increasingly rely on these systems to drive user engagement, the line between passive intermediary and active publisher becomes blurred, challenging the applicability of Section 230 in its original form.

6.2. Revenue Sharing and Complicity in Harmful Content

Another significant aspect of the *Gonzalez* case is the family's allegation that YouTube's revenue-sharing system allowed ISIS to benefit financially from its content. This claim attempted to extend liability beyond content moderation to the financial operations of the platform, suggesting that YouTube's model of sharing ad revenue with content creators made it complicit in supporting terrorism. However, the court found that the plaintiffs failed to provide evidence of any direct agreement or intent between Google and ISIS, a necessary element for establishing secondary liability or conspiracy under anti-terrorism laws.

While the court dismissed these allegations, the broader issue is: Should platforms that financially benefit from user-generated content, especially harmful content, be held accountable for the consequences of such content? Revenue-sharing models, which incentivize engagement farming, could be seen as indirectly encouraging the spread of harmful material. This raises important ethical questions about the responsibility platforms bear not only for hosting content but for profiting from it.

6.3. Arguments on Section 230 of the CDA

One of the biggest arguments against the reformation of Section 230 is that a change to Section 230 is a threat to free speech or the First Amendment and Fourth Amendment (Electronic Frontier Foundation, n.d.). Kosseff (2019) opined that Section 230's current protections enable online platforms to host user-generated content without fear of facing legal liability for that content. Revising Section 230 therefore could lead to platforms implementing more aggressive content moderation policies out of fear of legal repercussions, thereby limiting open discourse online. Well, true. However, according to Citron & Franks (2020), this is an overly simplistic interpretation as the interpreters treat all internet actions and interactions as speech protected under the First Amendment, disregarding the nuances of what types of speech actually receive constitutional protection. They posit that not every form of speech enjoys protection under the First Amendment —only that which addresses matters of public concern or contributes to public discourse. This means not all content shared on the internet is automatically deserving of protection under the banner of free speech.

Going further, there is another critical point to address - the role of algorithms in shaping the visibility and distribution of user-generated content. If we categorize all interactions on the internet as forms of speech, would this not also include the algorithmic processes that determine what content is amplified or suppressed? If algorithms are considered speech, then Section 230's immunity provisions create a contradiction. The immunity protects platforms from legal liability for user-generated content, but it also shields them from accountability for how their algorithms manipulate the distribution of that content, which has significant real-world implications.

Algorithmic decision-making is not neutral (Noble, 2018). It influences what content users see, how often they see it, and in what context. If platforms are allowed to shape the flow of information without any accountability, they essentially wield unchecked power over public discourse. This has already been evidenced by the spread of harmful content, disinformation, and radicalization online, where algorithms—designed to maximize engagement—often prioritize sensational content over balanced discourse. By not holding platforms accountable for the impact of these algorithmic processes, we ignore the reality that the design and implementation of algorithms are intentional decisions, not neutral or passive processes.

On the other hand, if algorithms are *not* considered speech, then we face a different issue- a discrepancy in the legal treatment of online content. User-generated content is subject to algorithmic processes- which, more often than not dictate its visibility and reach- yet platforms are absolved of responsibility for how their algorithms amplify or suppress that content. This creates a gap where platforms can evade accountability for redistributing harmful content or misinformation, under the guise of Section 230 immunity. Either way, it hits back to platform algorithms.

So, what can be done? A middle ground is needed—one that preserves the core principles of free speech while acknowledging the need for platform accountability in an algorithmic era. Reforming Section 230 does not have to mean stifling open discourse; rather, it could introduce protections that differentiate between platforms' passive hosting of content and their active role in how their algorithms influence user engagement and content visibility, particularly when such processes lead to the amplification of harmful or misleading information

6.4. Alternative Strategies

Discourse on the reformation of Section 230 of the CDA is not new. A lot of authors have pointed out the oversimplification in the interpretation of Section 230 of the CDA to modern internet dynamics. Most notably, scholars like Citron and Wittes (2017) have gone deep to propose alternative strategies that will introduce a degree of reasonableness to the protection Section 230 offers. In particular, Citron and Wittes (2017) opine that instead of focusing solely on broad censorship or content moderation, we could shift our attention to the underlying speech acts that occur on online platforms. Their stance highlights the importance of considering the context in which online communication takes place. This includes not only the specific words or images being shared but also the intent behind them, their potential impact on others, and the social dynamics at play within online communities. With this, we can better address the harmful effects of online behavior such as harassment, hate speech, and misinformation. This also means that the principles of free expression are upheld while still addressing harmful behavior. To them, while Section 230 was originally intended to protect online platforms from liability for user-generated content, it has also shielded platforms from accountability for their own harmful actions or inaction. Therefore, Section 230 reform should aim to exclude platforms that engage in bad faith practices, such as knowingly hosting illegal content, facilitating harassment or discrimination, or profiting from harmful activities.

In addition to what has been discussed, it is important to reiterate that Section 230's recognition of platforms as ‘publishers’ means they are viewed as mediums for communication, not as speech itself. However, the internet today is far more advanced than it was in 1996 when Section 230 was originally conceived. As inferred from the *Gonzalez v. Google* case and other related discussions, one key suggestion is to introduce new legal and ethical standards specifically for algorithmic content recommendation systems.

Therefore, instead of the blanket immunity currently granted by Section 230, a more balanced approach would be to implement conditional immunity. This immunity would be contingent upon platforms fulfilling certain conditions, such as:

Algorithmic transparency requirements: Most users have little understanding of how their data is used, aggregated, traded and how algorithms shape their online experiences. By implementing **algorithmic transparency**, platforms would be required to disclose how their algorithms function, which will make the decision-making processes behind content dissemination more visible. This will promote **accountability**, as it allows users, regulators, and researchers to examine algorithmic practices and hold platforms responsible for any negative impacts, such as the amplification of harmful content.

Establishment of data ownership rights: As I have argued earlier, people whose data are being traded for profit with little to no accountability should at least have the right to own and control their personal data, including use and non-use. Data ownership rights empower users and their agency to assert control over how their data is collected, processed, and used by online platforms. This also creates a framework for holding platforms accountable for the responsible handling and protection of user data, to mitigate risks related to data breaches, unauthorized access, and exploitation. Data ownership rights simply represent an important step towards rebalancing the relationship between users and online platforms.

Establishing frameworks for the ethical use of data: Beyond setting up data ownership rights, there should be ethical guidelines for the collection and use of personal data, with a focus on minimizing data collection and making sure that data is used in ways that are consistent with user expectations and values. These platforms should also be required to provide users with clear and accessible information about their data practices, including how their data is collected, used, and shared.

Establishment of privacy-enhancing technologies (PETs): Another suggestion is the use of strict privacy-enhancing technologies (PETs), such as encryption and anonymization, to protect user data. PETs can help to ensure that personal data is kept private and secure, even when it is collected and processed by online platforms. By integrating these technologies into their systems, platforms can offer users greater privacy protection while still providing useful services.

All of these in addition to what Citron and Wittes (2017), have suggested would bring an alternative solution to Section 230 in a way that holds platforms responsible and protects the users, without conflicting with or opposing the First Amendment.

7. Conclusion

This paper discusses the limitations of Section 230 in protecting individual privacy in the age of surveillance capitalism. Through an analysis of legal precedents like the *Google v. Gonzalez* case, it has been shown that the broad immunity granted to online platforms under Section 230 is insufficient in addressing the privacy challenges posed by modern digital platforms. The rise of surveillance capitalism, marked by the extensive collection and exploitation of personal data, has further worsened these challenges.

The discussions in this paper have significant implications for policymakers, tech companies, and platform users. Policymakers must consider targeted reforms to Section 230 that narrow the scope of immunity and introduce new standards for algorithmic content recommendation systems. Tech companies should adopt privacy-centric technological solutions and ethical frameworks that prioritize transparency, accountability, and user empowerment. For platform users, these changes are important in guaranteeing that their privacy rights are upheld.

References

[1] Chisnall, M. (2020). Digital slavery, time for abolition? Policy Studies, 41(5), 1–19. https://doi.org/10.1080/01442872.2020.1724926.

[2] Citron, D. K., & Franks, M. A. (2020). The internet as a speech machine and other myths confounding Section 230 reform. Boston University Law Review, 87, 233-256. https://scholarship.law.bu.edu/faculty_scholarship/836/

[3] Citron, D. K., & Wittes, B. (2017). The internet will not break: Denying bad Samaritans Section 230 immunity. Fordham Law Review, 86(2), 401-429.

[4] Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. Television & New Media, 20(4), 336–349.

[5] Cotter, K. (2019). Playing the visibility game: How digital influencers and algorithms negotiate influence on Instagram. New Media & Society, 21(4), 895-913.

[6] Electronic Frontier Foundation. (n.d.). Section 230: The most important law protecting internet speech. https://www.eff.org/issues/cda230

[7] Fortunati, L. (2002). The mobile phone: Towards new categories and social relations. Information, Communication & Society, 5(4), 513–528. https://doi.org/10.1080/13691180208538803

[8] Gonzalez v. Google LLC. Oyez. https://www.oyez.org/cases/2022/21-1333 (Accessed April 8, 2024).

[9] Kosseff, J. (2019). The twenty-six words that created the internet. Cornell University Press.

[10] Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society, 23(1), 128-147.

[11] Solove, D. J. (2009). Understanding privacy. Harvard University Press.

[12] Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

[13] Twitter, Inc. v. Taamneh. Oyez. https://www.oyez.org/cases/2022/21-1496 (Accessed April 8, 2024).

[14] Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.