§230, Online Identity, and Linkable Pseudonymity

Tylar Bloch

CPSC 610 –Topics in Computer Science and Law
Yale University
December 2019

The gaps in §230 begin to surface:

In recent legal history, courts have continued to uphold the broad-sweeping immunity provided by §230 of the Communications Decency Act (CDA). Many of these courts have treated §230 as a valid policy decision that shields online platforms from the liabilities that arise from third-party content. As a result, courts have been limited in how they interpret §230, and thus limited in what they can do to help the victims of online crimes seek redress for the injuries. But as we see from many of these legal battles, online anonymity poses additional challenges to victims, who must know the culprit's identity in order to press charges.

Two court cases in particular, *Zeran v. American Online Inc.* and *Carafano v. Metrosplash*, best highlight this tension between §230 and online anonymity. In each case, the plaintiff was a victim of online defamation and invasion of privacy, and could not identify the person who wronged him/her. For this reason, both plaintiffs sought to hold the online platforms accountable for failing to remove the fictitious accounts in a timely manner. Yet in each case, the court affirmed that §230 protected online platforms from third-party liability, even when that party is unidentifiable. As the court articulated in *Zeran v. American Online Inc.*, §230 was drafted to uphold free expression, and not to curb injurious online behavior:

> While Congress acted to keep government regulation of the Internet to a minimum, it also found it to be the policy of the United States 'to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer' Id §230(b)(5). Congress made a policy choice, however, not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages.[1]

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

Similarly, in *Carafano v. Metrosplash*, the court held that an interactive computer service "qualifies for immunity so long as it does not also function as an 'information content provider'.[2]

As we see from these cases, when §230 is coupled with online anonymity, plaintiffs tend to find themselves in a double bind: they cannot hold online platforms liable given §230 protections, nor can they press charges against the unidentified sources that wronged them. For this reason, I argue that §230 is largely incompatible with pure online anonymity, and that we need to refine our current scheme surrounding online identity; for we must grant the victims of anonymous cybercrime with some legitimate means to seek redress for their injuries. And while many argue that we should nix §230 to reach the same goal, I believe that §230 is too ingrained in our technological landscape to completely get rid of. In his book *The Twenty-Six Words that Created the Interet*, Jeff Kosseff explains that while §230 is imperfect, it has produced a net benefit to society that we should aim to preserve:

> The Internet is not as exceptional as it was in 1996 because it is now woven into the fabric of nearly every aspect of life. It also is more complicated…but those are not reasons to eliminate Section 230. Instead, that is why we must preserve it; to eliminate Section 230 would remove the foundation from underneath the trillion-dollar industry that the section created.[3]

While many have also doubted whether changing the online identity landscape will have a large impact on cybercrime, as I will argue in this paper, we can change the norms surrounding our online activity by holding people more accountable; and this, in turn, can curb reckless behavior across the Internet, particularly across social media platforms.

<u>The digital identity emerges:</u>

---

[2] *Carafano v. Metrosplash*, 339 F.3d 1119 (9th Cir. 2003)
[3] Kosseff, J. (2019). *The Twenty-Six Words that Created the Internet*. Cornell University Press.

Anonymity has existed for hundreds, if not thousands, of years, and has allowed many to avoid the "stigma of authorship"[4] surrounding printed materials. Apart from the traditional "nom de plumes" of many American and European writers, people have historically sought anonymity for reasons ranging from free expression and privacy to whistleblowing and political dissidence. Because anonymity is so closely related to free speech, U.S. courts have increasingly acknowledged that there exists some implicit right to communicate anonymously. According to the court in *McIntyre v. Ohio Elections Commission,* in which a plaintiff challenged the constitutionality of a statute that barred the distribution of anonymous campaign literature, the First Amendment guarantees the freedom to publish anonymously:

> Anonymity is a shield from the tyranny of the majority…It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation…at the hand of an intolerant society.[5]

Put differently, the court argued that implicit in the free speech protections guaranteed by the First Amendment is the ability to freely choose whether to attach one's name to a piece of literature.

On the other hand, online anonymity and online anonymity is a relatively recent phenomenon. The ability to split ourselves between the physical and the virtual existed only after the birth of the Internet, where we could fabricate or curate our digital presence and become someone new. This notion of the "connected life", or "life through the lens of technology"[6], gives people a new form of agency, one in which they may redefine their identity based on the

---

[4] Paku, Gillian. "Anonymity in the Eighteenth Century." *Oxford Handbooks*, 15 June 2017, https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199935338.001.0001/oxfordhb-9780199935338-e-37

[5] *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995).

[6] "Technology: Virtual vs. Real Life: You Choose." *Psychology Today*, Sussex Publishers, https://www.psychologytoday.com/us/blog/the-power-prime/201105/technology-virtual-vs-real-life-you-choose

information they choose to provide or not provide to the world; for when we conceal our physical identity online, we may be inclined to act in ways we we normally wouldn't. According to one study out of the University of North Florida, when internet users retained anonymity, they "showed evidence of increased tendencies to aggress"[7]. Similar to the psychological concept of deindividuation, the trends surrounding anonymous online activity indicate that when we forge digital identities, we may lose the self-awareness present in our physical, everyday decisions.

For this reason, we must treat online anonymity as separate from other modes of anonymity. While court decisions like the one in *McIntyre v. Ohio Elections Commission* refer to physical anonymity (such as omitting one's name from a piece of literature), courts have largely remained silent with respect to a right to speak anonymously online:

> If one thing is clear, it is that there is no clarity. State and federal courts will continue to issue a mish-mash of conflicting opinions that provide little consistency or certainty for online speech. The U.S. Supreme Court, which is the final arbiter of all things constitutional, has not ruled the right to anonymous online speech.[8]

And perhaps this is because courts have still not ruled on whether one has a right to engage in online speech. In the case *Packingham v. North Carolina*, the court ruled that a statue barring sex offenders from social media was not narrowly tailored, though it balked at establishing a full-fledged "right to social media"[9]. In this respect, even if courts have reached a consensus concerning physical anonymity, there is insufficient evidence to conclude that the Constitution recognizes a right to anonymity online.

---

[7] Zimmerman, Adam G. "Online Aggression: The Influences of Anonymity and Social Modeling." *American Psychological Association*, American Psychological Association, 2012, https://psycnet.apa.org/record/2014-24373-001.

[8] "Do We Have a Right to Online Anonymity?" *The Reporters Committee for Freedom of the Press*, https://www.rcfp.org/journals/news-media-and-law-winter-2014/do-we-have-right-online-ano/.

[9] Lapowsky, Issie. "The Supreme Court Just Protected Your Right to Facebook." *Wired*, Conde Nast, 19 June 2017, https:/www.wired.com/story/free-speech-facebook-supreme-court/.

Still, we must recall that there are many different levels of online identity. Besides pure anonymity and open identity, partial anonymity and linkable pseudonymity are two variants of online identity that attempt to combine openness with privacy. While partial anonymity entails leaving out essential aspects of a person's identity, in linkable pseudonymity, people appear anonymous but ultimately can be reidentified under certain circumstances. And as Gary Marx explains, a person may be reidentified even when he or she does not have a unique identity:

> Modern technology offers a variety of ways of uncoupling verification from unique identity. Validity, authenticity, and eligibility can be determined without having to know a person's name or location. Public policy debates will increasingly focus on when verification with anonymity is, or is not, appropriate and on various intermediary mechanisms that offer pseudonymous buffers but not full identification.[10]

Understanding these distinctions is critical to creating policies around online anonymity, and, as I will argue in this paper, linkable pseudonymity is best equipped to address the holes present in §230.

<u>The goals of implementing a linkable pseudonymity regime:</u>

Also known as "revocable anonymity"[11], linkable pseudonymity implies that even if a person wishes to hide her identity, it can be traced back to her through various cryptographic and database access protocols. In systems of linkable pseudonymity, the most basic implementation is as follows:

> (1) Bob signs up on Platform, and stores identifiable information in Platform's database.
>
> (2) If Bob wishes to appear anonymous, and if the platform's policies permit it, the platform will encrypt Bob's information and store it in a database.

---

[10] Marx, Gary T. "Identity and Anonymity: Some Conceptual Distinctions and Issues for Research." *Identity and Anonymity*, MIT, 2001, https://web.mit.edu/gtmarx/www/identity.html

[11] Köpsell, Stefan, et al. *Revocable Anonymity*. 2006, *Revocable Anonymity*

(3) Alice files a civil claim to a local court.

(4) Local court judge reviews the claim, and issues an injunction for Platform to disclose Bob's identity

(5) Platform receives the injunction, decrypts Bob's identity, and sends it to both the court and Alice.

(6) Alice sues Bob in civil court.

Note that this scheme for linkable pseudonymity operates uniquely for civil claims, of which most exist as torts such as defamation, invasion of privacy, and intentional infliction of emotional distress.[12] Additionally, note that Alice does not have to be a member of said Platform to file a claim to the local court. And while this paper will not delve into technical details, it will address important theoretical aspects of implementing such a system.

Most importantly, a linkable pseudonymity regime grants cyber-victims the opportunity to confront their attackers in court. As we have seen in cases of anonymous defamation, "online anonymous defamation can cause serious harm to a business or person resulting in massive financial losses and permanent reputational injury".[13] While judges can sometimes subpoena Internet service providers (ISPs) to reveal the IP address of the person who made the defamatory post, courts generally dislike involving ISPs when the conflict exists uniquely on a specific platform or website. And because judges assume that online anonymity is difficult to circumvent, they often raise the bar for the evidence "sufficient to create a prima facie case on the elements of the claim"[14]. Lawyer Heater Saint summarizes this problem in her paper "Section 230 of the Communications Decency Act: The True Culprit of Internet Defamation:

---

[12] "Tort." *Legal Information Institute*, Legal Information Institute, https://www.law.cornell.edu/wex/tort.
[13] "Fighting Back Against Anonymous Defamation on the Internet: ten Steps to Take (United States)." *Association of Corporate counsel (ACC)*, https://www.acc.com/resource-library/fighting-back-against-anonymous-defamation-internet-ten-steps-take-united-states
[14] Levy, Paul Alan. "Litigating Civil Subpoenas to Identity Anonymous Internet Speakers." *Public Citizen*, https://www.citizen.org/article/litigating-civl-subpoenas-to-identify-anonymous-internet-speakers/.

> If someone posts a defamatory statement about someone on an AOL message board, AOL is protected, but the person who created the defamatory statement is subject to liability. Due to the anonymity offered by the internet, however, plaintiffs, more often than not, struggle to identify who authored the defamatory speech against them, which explains why they go after the ISP for retribution.[15]

A linkable pseudonymity regime, however, standardizes the process for this kind of civil litigation by putting each user's identity reasonably within the court's reach. Moreover, by keeping ISPs out of the picture, the court may engage only with posts on a particular platform, and thus avoids recklessly "fishing"[16] for evidence unrelated to the plaintiff's claims.

Furthermore, this regime skirts many of the conflicts raised by §230 by precluding plaintiffs from directly suing technology platforms. While §230 is still in place, platforms have little incentive to disclose its users' identities, and cannot be accountable for much of the harm that arises. On the other hand, with linkable pseudonymity, people can avoid this liability dispute by bringing anonymous users out of the dark when there is evidence that they have wronged others. When platforms adopt this protocol, they assume no further responsibility as publishers or distributors, and merely help users mediate disagreements more effectively. Accordingly, even with linkable pseudonymity, §230 can achieve its original purpose of immunizing platforms from third party content —all while dissuading users from suing the platforms themselves.

Notwithstanding, users can remain anonymous to the rest of the world so long as they tether their real identities to their online accounts in some capacity. Many argue that these users

---

[15] Saint, Heather. "Section 230 of the Communications Decency Act: The True Culprit of Internet Defamation." *Digital Commons at Loyola Marymount University and Loyola Law School*, https://digitalcommons.lmu.edu/elr/vol36/iss1/2/.

[16] "Fishing Expedition." *Legal Information Institute*, Legal Information Institute, https://www.law.cornell.edu/wex/fishing_expedition.

cannot truly be anonymous, and I concede that this form of anonymity is "conditional" at best. But those who accept nothing less than total anonymity, as the decision in *McIntyre* seems to suggest, mistakenly treat the Internet as a natural extension of more traditional forms of media like newspapers and televisions. In doing so, they permit users to share, curate, and consume content at an infinitely large scale, without first appreciating the "full dimensions and vast potential" of "the Cyber Age".[17] On this view, a linkable pseudonymity regime can serve as an effective safety net for internet communication by transforming the norms surrounding online behavior. That is, in keeping virtual and physical identities closer together, it can help users to participate in online communities more sensibly.[18]

The challenges of implementing a linkable pseudonymity regime:

Yet there are serious challenges to adopting such a system that span across many institutions: legal challenges, technological challenges, political challenges, and international challenges. To fully assess the possibility of implementing this regime, we need to explore each of these challenges separately.

A. Legal Challenges

As one option for implementing a linkable pseudonymity protocol, Congress could pass a statute mandating social media companies to collect from its users personally identifiable information (PII). For tech platforms that allow users to log in or post anonymously, they would be required to encrypt the information and store it in a private database. In this scenario, platforms including Twitter, Reddit, and Tinder would likely push back against the onerous

[17] Post, D. (2019, March 29). Opinion | Supreme Court unanimously overturns North Carolina's ban on social-media use by sex offenders. Retrieved from https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/03/supreme-court-unanimously-overturns-north-carolinas-ban-on-social-media-use-by-sex-offenders/.

[18] Dawson, J. (n.d.) Who is That? The Study of Anonymity and Behavior. Retried from https://www.psychologicalscience.org/observer/who-is-that-the-study-of-anonymity-and-behavior.

mandates, arguing that their users have a right to participate anonymously, a right that has proven vital to their business models. As Reddit's CEO Steve Huffman explained 2018, "privacy is built into Reddit", and that "when people detach from their real-world identities, they can be more authentic, more true to themselves."[19] These privacy-centric companies have come to appreciate the separation between virtual and physical identities, and would likely fight hard to preserve that which makes their platforms "authentic".

Accordingly, before Congress could pass this statute, courts would need to first agree on whether a right to online anonymity exists. While many including the Electronic Frontier Foundation argue that the court's decision in *McIntyre* ought to apply to online speech, others believe that the Internet is so revolutionary that it cannot yet house every protection granted by the First Amendment. In her article "Applying McIntyre v. Ohio Elections Commission to Anonymous Speech on the Internet", lawyer Caroline Strickland argues that there are four key qualities—immediate impact, ease of access, remote operability, and normative anonymity—that distinguish online communication from physical speech:

> These qualities increase the potential for harm from false Internet speech; thus, courts should consider the Internet's unique nature when evaluating requests for expedited discovery.[20]

Though Strickland acknowledges that anonymity serves an important role on the Internet, she stresses that courts must not ignore the medium through which speech is conveyed, for it can impact the magnitude and variety of harm a cyber-victim experiences.

---

[19] Gutman, R. (2018, July 3). Reddit's Case for Anonymity on the Internet. Retrieved from https://www.teatlantic.com/technology/archive/2018/06/reddit-anonymity-privacy-authenticity/564071/.
[20] Caroline E. Strickland, "Applying McIntyre v. Ohio Elections Commission to Anonymous Speech on the Internet and the Discovery of John Doe's Identity", 58 Wash. & Lee L. Rev. 1537 (2001), https://scholarlycommons.law.wlu.edu/wlulr/vol58/iss4/13

Additionally, courts would need to affirm or dismiss the five-part test in *Dendrite International, Inc. v. Doe No. 3*, a protocol to help courts determine whether to mandate the disclosure of an anonymous blogger's identity.[21] The five-part test reads:

> (1) The plaintiff must make good faith efforts to notify the poster and give the poster a reasonable opportunity to respond.
>
> (2) The plaintiff must specifically identify the poster's allegedly actionable statements.
>
> (3) The complaint must set forth a prima facie cause of action.
>
> (4) The plaintiff must support each element of the claim with sufficient evidence.
>
> (5) The court must balance the defendant's First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous defendant's identity.

While this test grants to courts the ability to compel technology platforms or Internet service providers to reveal a suspect's identity, it presents serious hurdles to those seeking to rectify their harms. In particular, the test fails to address precisely how much evidence plaintiffs must show to substantiate their claims. Establishing that evidence must be "sufficient", though logical and concise, is so vague that courts are left to guess if and under what circumstances online posts themselves can sufficiently substantiate the plaintiff's claim. Additionally, the *Dendrite* test presumes a "right of anonymous free speech" that may not exist online. As previously discussed, courts, including the Supreme Court, have hesitated to conclude whether Internet users have a right to consume and share content anonymously.[22] Accordingly, for the *Dendrite* test to become legitimate, courts would need to first establish whether they can compel private companies to reveal the identities of its users in civil suits.

B. Political Challenges

[21] *Dendrite International, Inc. v. Doe No. 3*, 342 N.J. Super. 134, 775 A.2d 756

[22] "Do We Have a Right to Online Anonymity?" *The Reporters Committee for Freedom of the Press*, https://www.rcfp.org/journals/news-media-and-law-winter-2014/do-we-have-right-online-ano/.

Before the statute could pass, however, Congress would need to overcome political hurdles concerning surveillance and privacy. Many pro-privacy groups like the ACLU fear that collecting users' personally identifiable information creates a serious liability for technology companies, and further incentivizes law enforcement to investigate suspects' online activity:

> New technologies are making it easier for governments and corporations to learn the minutiae of our online activities. Corporations collect our information to sell to the highest bidder while an expanding surveillance apparatus and outdated privacy laws allow the government to monitor us like never before.[23]

These concerns reflect our current political climate surrounding "big data", and its accompanying threats to human security[24]. Granted, anytime we collect data, there are risks of data breaches and data malpractices, and we magnify these risks by collecting data on a larger scale. For this reason, the statute would have to explicitly state how and under what circumstances courts can mandate the disclosure a user's identity. Likewise, the statute would have to require companies to follow specific protocols in encrypting the information. These challenges are non-trivial, and would require that legislators and computer scientists collaborate extensively.

In addition, policymakers would have to decide what information should be required, and whether to verify that information. Many look to the flaws of Facebook's "real-name" policy as evidence that efforts to prevent online trolling are ultimately ineffective.[25] Even with this policy, Facebook reported last year that it had taken down 2.8 billion fake accounts, many of which were

---

[23] "Internet Privacy." *American Civil Liberties Union*, https://www.aclu.org/issues/privacy-technology/internet-privacy.
[24] Mavriki, Paola, and Maria Karyda, "Big Data Analytics: From Threatening Privacy to Challenging Democracy." *SpringerLink*, Springer, Cham, 12 Dec. 2019, https://link.springer.com/chapter/10.1007/978-3-030-37545-4_1.
[25] "What Names Are Allowed on Facebook?: Facebook Help Center." *Facebook*, https://www.facebook.com/help/112146705538576.

duplicate accounts or bots.[26] Because Facebook does not require its users to submit a valid government issued ID in order to register, people can more easily create accounts with fake names and fake personal information. Given that social media platforms would have to verify its users' information to crack down on anonymous trolls, the statute would have to propose how and to what extent these platforms must adopt this protocol.

Policymakers would also have to be mindful that this scheme will hurt the technology sector by raising the costs of using its services. People who use these platforms knowing that they can remain purely anonymous would lose this privilege, and might consider pulling out as a result. In this regard, the statute would have to enforce real-name registration without greatly raising the barrier to entry for social media users. And because many claim that adopting real-name registration will hurt undocumented migrants[27], policymakers should aim to restrict access to the data to only individuals and courts. That is, the statute should keep organizations with potentially malicious intentions like Immigration and Customs Enforcement from exploiting this information.

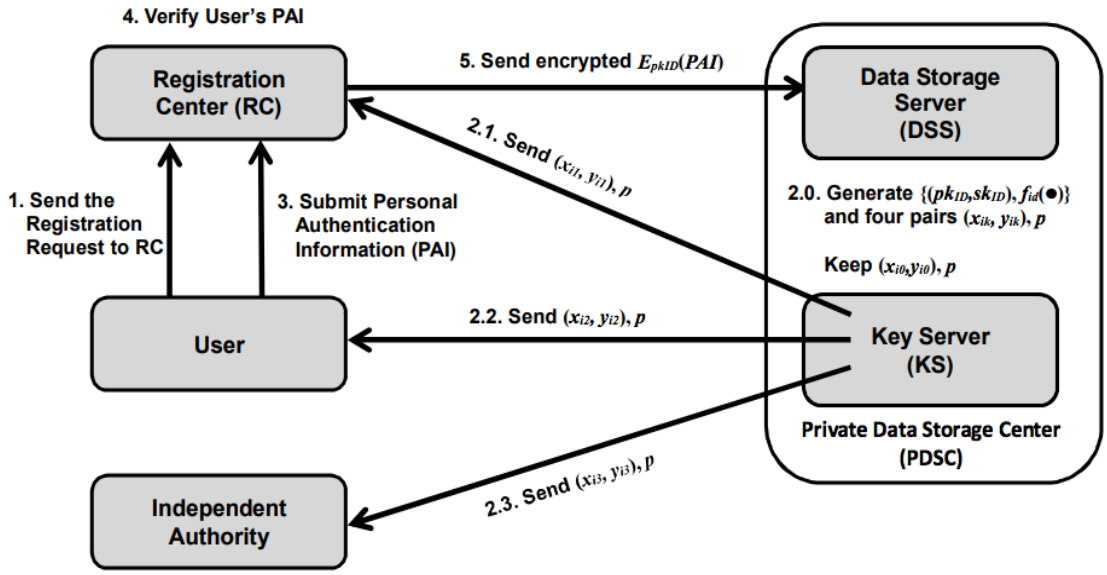
C. Technological Challenges

For the statute to be effective, social media companies would need to encrypt and manage the data according to clear guidelines. As discussed earlier, many fear that aggregating data in the private sector will lead to mass surveillance. For this reason, the statute would have to standardize how private companies encrypt the data, perhaps through public key cryptography. According to one cryptographic scheme for real-name registration, users can submit their

---

[26] Nicas, Jack. "Does Facebook Really Know How Many Fake Accounts It Has?" *The New York Times*, The New York Times, 30 Jan. 2019, https://www.nytimes.com/2019/01/30/technology/facebook-fake-accounts.html.
[27] "Inclusive Approach to Immigrants Who Are Undocumented Can Help Families and States Prosper." *Center on Budget and Policy Priorities*, 9 Sept. 2019, https://www.cbpp.org/research/state-budget-and-tax/inclusive-approach-to-immigrants-who-are-undocumented-can-help.

information to a registration center after having been provided with a public-private key pair, and then send the encrypted message to a data storage server:[28]



Most importantly, an independent authority (i.e. the technology company) will have to maintain the public-private key pairs, and readily access them when courts present them with a valid injunction. Yet regardless of the scheme policymakers and computer scientists agree upon, social media companies will have to ensure the confidentiality, integrity, and availability of the personally identifiable information. They will have to safely store data in an encrypted database while allowing the private key manager to decrypt a user's information when necessary.

Granted, large technology companies will be able to implement such a system more easily than smaller startups can. Generally, whenever businesses operate on a larger scale, they can more easily hire the labor and accumulate the capital to comply with federal standards[29] —not to

[28] Xu, Fei et. al. "A Privacy-Preserving Encryption Scheme For an Internet Real-Name Registration System". 11th IFIP International Conference on Digital Forensics (DF), Jan 2015, Orlando, FL, United States.
[29] Buchanan, Leigh. "When It Comes to Regulations, the Deck is Stacked Against Small Businesses." *Inc.com*, Inc., 8 Sept. 2017, https://www.inc.com/leigh-buchanan/why-the-government-needs-a-whole-different-set-of-rules-for-small-businesses.html.

mention the computing power necessary to maintain such large databases. Consequently, policymakers must aim to keep the costs of implementing these technologies low, else the regulation will disproportionately burden smaller businesses.

D. International Challenges

Because social media platforms attract users from around the globe, many anonymous accounts correspond to foreign IP addresses. This aspect of online communication makes it difficult for American cyber-victims to rectify injuries caused by foreign suspects. Even if courts are able to issue injunctions to disclose the identity of the anonymous user, the victim would have to sue the user outside the U.S. Additionally, social media platforms will have a harder time collecting and verifying personally identifiable information from abroad. If an Italian wishes to become a Reddit user, under this scheme, he would have to comply with the platform by submitting the necessary information. Accordingly, social media companies would have to prepare themselves to review diverse data sets, especially if they require valid government-issued identification.

This challenge reflects the growing issue of state sovereignty in the digital age. On the Internet, users are constantly complying with other states' laws and regulations, even if they are operating remotely. In this regard, many believe that the internet is eroding physical borders, leading to weak enforcement over global communication.[30] While a single statute could not solve this entire problem, states that wish to address the problem of anonymous trolls must collaborate, perhaps drafting international treaties to centralize all conflicts that exist among Internet users.

Conclusion:

[30] "Is the Internet Eroding State Sovereignty?" *FutureLearn*, https://www.futurelearn.com/courses/global-citizenship/0/steps/32103.

Over the past decade, online anonymity has proven incompatible with §230. Because §230 immunizes technology platforms from the intermediary liability that arises from third-party content, companies have little incentive to disclose its users' identities in civil cases. As a result, users who are wronged by anonymous suspects are largely unable to rectify their injuries. These anonymous trolls have continued to enjoy the expanded reach and remote operability that the Internet enables, creating virtual identities that lack the same inhibitions that drive their in-person interactions. While courts have interpreted from the First Amendment a right to speak anonymously, they have been reluctant to apply this right to cyberspace. Though the court in *Packingham* equated social media to the "modern public square"[31], internet communication has continued to evolve into a new species of self-expression, creating new challenges for courts and for content moderators who wish to protect users from harm.

To respond to these issues, governments should strongly consider enforcing a linkable pseudonymity regime for social media platforms. Linkable pseudonymity can benefit society in four primary ways: (1) by keeping physical and virtual identities closer together and altering the norms surrounding online conduct, which keeps users more accountable for their actions; (2) by allowing cyber-victims to directly confront their attackers in court; (3) by reducing the need to issue subpoenas to ISPs, which often leads to "fishing expeditions" for unrelated evidence; and (4) by keeping people from suing the platforms themselves, a costly move that consistently proves fruitless under the current §230 paradigm. To reach these goals, however, policymakers and computer scientists will have to overcome a series of challenges, challenges that require considerable legal, political, technological, and international insight.

---

[31] *Packingham v. North Carolina*, 582 U.S. ___ (2017)

§230 has fundamentally transformed the tech industry, though not without its costs. It has left the victims of anonymous harassment and defamation without legal recourse, ultimately unable to hold the platform or the anonymous accountable. Linkable pseudonymity, however imperfect it may be, can help to revive in online communication the integrity and mindfulness that make in-person communication so valuable. While courts still have to determine whether there exists a right to engage in online expression, policymakers will have to determine whether the five-prong *Dendrite* test is effective enough to uphold. Regardless of whether such a statute might pass, deciding these matters will invariably prove helpful in creating policies that affect the future of online expression.