# NetChoice and Section 230: The future of online content moderation in the United States

**Yaron Dori**, **Megan Crowley** and **Diana Lee** of Covington analyse the potential importance of this case.

This term, the US Supreme Court will hear two cases, *Moody v. NetChoice, L.L.C.* (11th Cir.) and *NetChoice, L.L.C. v. Paxton* (5th Cir.), that could alter how social media companies moderate content, with potentially significant implications. Both cases concern state laws (in Florida and Texas, respectively) that restrict large social media companies from curating and moderating third-party content on their platforms, and impose certain related requirements. The plaintiffs in each case argue that the laws violate the First Amendment to the US Constitution, which prohibits, with certain exceptions, state and federal governments from imposing restrictions on speech.

Beyond the First Amendment considerations at play, an important backdrop to the *NetChoice* cases is Section 230 of the Communications Act, which immunizes online platforms from civil liability arising from third-party content on their platforms, and the removal of third-party content in certain circumstances. In this article, we provide a brief history of Section 230 and describe the potential implications of the *NetChoice* cases for this provision. In particular, we discuss the Section 230 issues that may inform the Supreme Court's consideration of the First Amendment issues in dispute, and the potential for Section 230 to take center stage in any future proceedings in these cases.

## Brief history of Section 230

Section 230 is a provision of the Communications Act that (1) immunizes providers and users of an "interactive computer service" from liability for content posted by others on the service; and (2) allows "interactive computer service" providers to moderate content on their services without jeopardizing that immunity.[1] Section 230 has been interpreted to apply to websites, applications, social media platforms, and other online services that host third-party content. For purposes of this article, we refer to such interactive computer services as "online platforms."

To understand Section 230's purpose, it is important to have an understanding of the state of the law before the Internet and before Section 230 was enacted.

## The law before Section 230

Subject to certain exceptions, the First Amendment prohibits the state and federal governments from restricting the exercise of speech. These protections apply to private entities, in addition to natural persons.[2] Before Section 230 was enacted, however, there were limits to the protections private entities could claim for hosting or providing third-party content. Although it was undisputed that the First Amendment protected speech by "publishers" or "speakers" of content, it was less clear whether the First Amendment also protected the "distributors" of such content, such as magazine distributors or booksellers.

In 1959, the Supreme Court struck down as unconstitutional an ordinance imposing strict liability on a bookseller who distributed obscene material, finding that the ordinance's failure to require any knowledge on the part of the bookseller would impose a "severe limitation" on the public's access to constitutionally-protected expression.[3] That case, *Smith v. California*, established that distributors of third-party content cannot be liable for content they distribute unless they *knew or had reason to know* that the content they were distributing was illegal. The Court explained that although "obscene speech and writings are not protected" speech under the First Amendment, punishing their distribution without regard to the distributor's knowledge of the infringing content would "have the collateral effect of inhibiting" the dissemination of other protected expression.[4]

Some argued that by placing the burden on the government to establish the distributor's mental state, *Smith v. California* incentivized distributors to remain ignorant of the content they were distributing. At the same time, others argued that *Smith v. California* was not sufficiently protective of distributors because anyone who objected to content the distributors carried could tell them that it was illegal, thereby "foisting" knowledge onto them.

The Internet magnified this dilemma, as illustrated by two cases: *Cubby v. CompuServe*,[5] and *Stratton Oakmont v. Prodigy*.[6] In *Cubby*, a court held that an online service provider could be liable for third-party content on its site only if it knew or should have known of the content's unlawfulness. By contrast, in *Stratton Oakmont*, a court concluded that by moderating its online message boards and deleting certain messages, an online provider became responsible for all third-party content on its site, regardless of its knowledge of lawfulness of that content.[7] Taken together, Cubby and Stratton Oakmont left online service providers with two options: (1) refrain from removing any third-party content from their platforms and avoid liability, but risk a "free for all" by users, or (2) moderate third-party content, but risk being held liable for that content.

## The legislative solution

In the mid-1990s, Congress was considering reforming the nation's telecommunications laws, in part due to concerns about the proliferation of pornography on the Internet. Against this backdrop, the dilemma posed by *Cubby* and *Stratton*

*Oakmont* became more apparent.

Partly in response to this dilemma, Congress enacted Section 230, which prevents online platforms from being "treated as the publisher or speaker" of third-party content on their sites, immunizes platforms from most civil liability for such content (even if the platforms knew or should have known about the unlawfulness of the content), and permits platforms to moderate content in good faith without losing that immunity.[8] Specifically, Section 230(c)(1) provides, "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." Section 230(c)(2) further provides that no provider or user of an interactive computer service shall be liable for any action "voluntarily taken in good faith" to restrict access to third-party content the provider or user "considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable."

Together, these provisions reflect their drafters' understanding that online platforms cannot possibly review all content on their sites, and if they could have knowledge of violating content foisted on them by others, this could stifle the internet's potential to become a vibrant marketplace of ideas.[9]

## The *NetChoice* cases

For years, courts interpreted Section 230 to afford online providers broad immunity for third-party content on their platforms. Recently, however, dozens of legislative proposals have been introduced to reform Section 230, with critics arguing that Section 230 immunity is too broad, shielding providers from liability for content for which, critics allege, the providers should be held liable.[10] At the same time, some state legislatures have enacted laws that restrict certain online providers from moderating third-party content on their sites. The *NetChoice* cases concern two such laws: Texas House Bill 20 (HB-20) and Florida Senate Bill 7072 (SB-7072).

**The NetChoice challenges to HB-20 and SB-7072:** Enacted in 2021, HB-20 and SB-7072 restrict large social media platforms' ability to moderate third-party content on their sites. Among other provisions, HB-20 prohibits large social media platforms from "censoring" content on the basis of viewpoint or geographic location within the state. "Censor" is defined as "to block, ban, remove, deplatform, demonetize, de-boost, restrict, deny equal access or visibility to, or otherwise discriminate against expression"—encompassing vast swaths of content moderation.[11] SB-7072 similarly prohibits large social media platforms from restricting the speech of political candidates and certain "journalistic enterprises."[12]

NetChoice, a trade industry group, challenged the laws, arguing, among other things, that they violate the First Amendment and are preempted by Section 230.[13] In May 2022, the Eleventh Circuit upheld a district court's injunction of SB-7072's content moderation provisions on First Amendment grounds, and a few months later, the Fifth Circuit reached the opposite conclusion, holding that HB-20's restrictions on content moderation did not violate the First Amendment. Neither court reached the Section 230 preemption issue.

**The Supreme Court's Review and potential implications for Section 230:** This term, the Supreme Court will consider the conflicting First Amendment decisions from the Fifth and Eleventh Circuits.[14] Although the Supreme Court granted *certiorari*[15] on only First Amendment questions, Section 230 may well figure into the Court's consideration of these cases in three ways.

First, the states have explicitly invoked Section 230 in their briefing to date, arguing that social media companies "cannot simultaneously demand First Amendment *protection* for [the] same conduct" for which they claim immunity under Section 230(c)(1).[16] In other words, the states' view is that if the companies claim immunity under Section 230 as distributors or "non-speakers" when they moderate content, they cannot also avail themselves of the rights of speakers under the First Amendment. The Fifth Circuit endorsed this argument in its decision, reasoning that Section 230 "reflects Congress's judgment that the Platforms are not acting as speakers or publishers when they host user-submitted content," and suggesting that as a general matter, Section 230 should be interpreted narrowly to permit online platforms to moderate content only in a narrow set of circumstances.[17] It is likely that the states will raise this argument in the merits-stage briefing before the Supreme Court.

There are substantial weaknesses, however, to the states' interpretation of Section 230. In particular, although Section 230(c)(1) provides that platforms will not be treated as speakers or publishers of third-party content for purposes of civil liability, that does not necessarily mean that platforms are not actual speakers for purposes of the First Amendment when they decide what third-party content to host on their sites. Indeed, such a conclusion appears to be contrary to Congress's intent in passing Section 230, which was in part to encourage online content moderation so that the Internet could become a vibrant marketplace of ideas.

Second, although the lower courts did not address plaintiffs' argument that the Texas and Florida laws are preempted by Section 230, if the Supreme Court upholds the laws under the First Amendment, preemption likely will become a key issue on remand.

Third, the text of HB-20 itself contains an explicit carve-out for federal law, which largely has not been addressed in the *NetChoice* briefing. That carve-out states that HB-20 "does not prohibit a social media platform from censoring expression" that, among other things, "the social media platform is *specifically authorized to censor by federal law*."[18] Litigants may argue that Section 230 "specifically authorize[s]" their content moderation activities, and therefore exempts them from HB-20's reach.[19]

## Conclusion

The Supreme Court's decision in NetChoice will likely have significant implications for First Amendment jurisprudence as it relates to online providers' ability to moderate third-party content on their sites, and may further complicate courts' understanding of the reach of Section 230.

**AUTHORS**

Yaron Dori and Megan Crowley are Partners, and Diana Lee an Associate at Covington, US.
Emails: ydori@cov.com
mcrowley@cov.com
dlee@cov.com

## REFERENCES


1 47 U.S.C. § 230(c). An "interactive computer service" is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. §230(f)(2).

2 See, e.g., *First Nat. Bank of Boston v. Bellotti*, 435 U.S. 765, 778-84 & n.14 (1978).

3 361 U.S. 147, 153 (1959).

4 *Ibid*. at 152.

5 776 F. Supp. 135 (S.D.N.Y. 1991).

6 23 Media L. Rep. 1794, 1995 WL 323710 (N.Y. Sup. Ct. 1995).

7 *Ibid.* at *4.

8 Section 230 does not immunize providers from criminal liability or for certain kinds of civil liability, such as intellectual property claims and violations of sex trafficking laws.

9 See *Batzel v. Smith*, 333 F.3d 1018, 1026-1030 (9th Cir. 2003) (describing the legislative history of Section 230).

10 See, e.g., *Gonzalez v. Google*, 598 U.S. 617 (2022).

11 Tex. Civ. Prac. & Rem. Code § 143A.001(1).

12 Both laws also require providers to give users individualized explanations if their content is removed or altered, and to make general disclosures about the providers' internal operations and content moderation policies. See, e.g., Fla. Stat. § 501.2041; Tex. Bus. & Com. Code Ann. §§ 120.103(a), 120.052, 120.053.

13 The doctrine of federal preemption is grounded in the Supremacy Clause of the U.S. Constitution, U.S. Const. art. VI, § 2, under which a federal law may "override[]" a state or local law when, for example, the two laws conflict. *Crosby v. Nat'l Foreign Trade Council*, 120 S. Ct. 2288, 2294-95 (2000) (internal citation omitted).

14 The Supreme Court's review of the *NetChoice* cases follows its decision in *Gonzalez v. Google*, LLC, 598 U.S. 617 (2023) (per curiam), in which the Court declined to consider whether YouTube may claim Section 230 immunity from a claim of secondary liability under the Anti-Terrorism Act (ATA) for its recommendation algorithms, holding instead that much of the plaintiffs' ATA complaint would fail to state a claim for relief under the Court's separate decision in *Twitter v. Tamneh*, 598 U.S. 471 (2023).

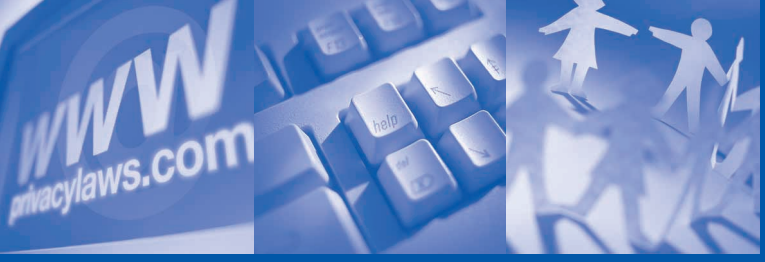
15 A formal order issued by a higher court to a lower court or tribunal, instructing them to submit the entire record of a case for review.

16 Suppl. Br. for Resp. at 4, *NetChoice, LLC v. Colmenero*, No. 22-555 (Aug. 28, 2023) (emphasis in original).

17 *NetChoice, L.L.C. v. Paxton*, 49 F.4th 439, 468 (5th Cir. 2022).

18 HB-20 § 143A.006(a) (emphasis added).

19 Indeed, HB-20's primary drafter has endorsed this view. See Mike Masnick, 'Author of Texas' Social Media Law Admits that He Meant the Law to Exempt Any Moderation Decisions Protected by Section 230 (That's Everything)', www.techdirt.com/2022/05/17/author-of-texas-social-media-law-admits-that-he-meant-the-law-to-exempt-any-moderation-decisions-protected-by-section-230-thats-everything/




ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

# Data protection enforcement trends in Germany

By **Julia Garbaciok** and **Katharina A. Weimer** of Fieldfisher.

In Germany there have been interesting recent decisions and trends across the country. In this article we discuss the latest news on e-marketing consent rules, and give an overview on recent developments in German employee data protection law, as well as a few highlights relating to data subjects' access rights requests.

*Continued on p.3*

# Creating an AI governance framework: US and EU take steps to lead

The EU is finalising its AI Act while the US adopts a Presidential Executive Order on AI and creates an Artificial Intelligence Safety Institute. How are companies preparing? By **Laura Linkomies**.

The EU is still in the middle of the Trilogue process between the European Parliament, the European Council, and the European Commission. In October, they agreed on wording addressing important classification rules for high-risk artificial intelligence (AI) systems, but there are still other aspects to be finalised. There will be a certification regime for high-risk AI systems, and the Commission now

*Continued on p.6*



Issue 186 **DECEMBER 2023**

INTERNATIONAL report

ISSUE NO 186 DECEMBER 2023

**PUBLISHER**
**Stewart H Dresner**
stewart.dresner@privacylaws.com

**EDITOR**
**Laura Linkomies**
laura.linkomies@privacylaws.com

**DEPUTY EDITOR**
**Tom Cooper**
tom.cooper@privacylaws.com

**ASIA-PACIFIC EDITOR**
**Professor Graham Greenleaf**
graham@austlii.edu.au

**REPORT SUBSCRIPTIONS**
**K'an Thomas**
kan@privacylaws.com

**CONTRIBUTORS**
**Julia Garbaciok and Katharina A. Weimer**
Fieldfisher, Germany
**Professor Graham Greenleaf**
UNSW, Australia
**Nana Botchorichvili**
IDEA Avocats, France
**David van Boven**
Privacy Lawyer, the Netherlands
**Patrick van Eecke, Loriane Sangaré-Vayssac and Enrique Capdevila**
Cooley, Belgium
**Yaron Dori, Megan Crowley and Diana Lee**
Covington, US
**Uche Val Obi San**
Alliance Law Firm, Nigeria
**Abigail Dubiniecki**
Privacy Consultant, Canada

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
**Tel: +44 (0)20 8868 9200**
**Email: info@privacylaws.com**
**Website: www.privacylaws.com**
**Subscriptions:** The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X



# comment

## Keeping up with AI is a challenge

There are so many privacy developments in AI governance. This issue will give you a good insight into some of the most recent news. The US Executive Order pushes the US to the lead in AI governance (p.1 and p.8) as the EU, with its complex decision-taking structure, has been delayed in adopting its AI Act. EU DPAs are alert and conduct their own investigations on AI but also unite at the European Data Protection Board to construct common positions. There is an important role for lawyers and DPOs now that market practices are developing. Privacy must be baked into products but also into organisations' AI governance, as our correspondent says.

But thoughtful public policy decisions are difficult to make when we do not fully understand the opportunities and risks with using AI, nor the impact on society as a whole.

Specifically working on privacy and new technologies is the International Working Group on Data Protection in Technology (the Berlin Group) which issues working papers on specific themes. The German-led group provided an update at the DPAs' Global Privacy Assembly in Bermuda, saying it works especially closely with the UK ICO and France's CNIL to develop future technology monitoring so that DPAs can issue privacy-friendly advice at an early stage of development of these technologies (www.bfdi.bund.de/EN/Fachthemen/Inhalte/Europa-Internationales/Berlin-Group.html).

In Bermuda, views were exchanged on the new EU-US Data Privacy Framework, which will inevitably face challenges (p.14), as well as enforcement cooperation, AI, risk based approaches and more (p.26).

We welcome your speaker offers in the first half of December for PL&B's 37th Annual Conference 1-3 July 2024 at St. John's College, Cambridge www.privacylaws.com/events-gateway/events/2024ic37/

As this is the last edition for 2023, I would like to thank you, our loyal readers, for your support and feedback (more needed though!). We are privileged to work with so many talented people, especially our *PL&B* Correspondents.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

## Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

# Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

## PL&B's International Report will help you to:

**Stay informed of data protection legislative developments in 180+ countries.**

**Learn from others' experience through case studies and analysis.**

**Incorporate compliance solutions into your business strategy.**

**Find out about future regulatory plans.**

**Understand laws, regulations, court and administrative decisions and what they will mean to you.**

**Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.**

## Included in your subscription:

**1. Six issues published annually**

**2. Online search by keyword**
Search for the most relevant content from all *PL&B* publications.

**3. Electronic Version**
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

**4. Paper version also available**
Postal charges apply outside the UK.

**5. News Updates**
Additional email updates keep you regularly informed of the latest developments.

**6. Back Issues**
Access all *PL&B International Report* back issues.

**7. Events Documentation**
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

**8. Helpline Enquiry Service**
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

**9. Free place at a *PL&B* event**
A free place at a *PL&B* organised event when booked at least 7 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

**privacylaws.com/reports**

> "An indispensable resource for anyone who has a serious interest in privacy, combining latest news with thoughtful commentary and analysis."
>
> **Richard Cumbley, Partner, Linklaters**

## UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the current Data Protection and Digital Information Bill, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business.

## Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

## Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.