

The “Platform-as-Actor” Doctrine: USMCA Chapter 19, Section 230, and the Limits of a Novel Intermediary-Liability Theory

Executive Summary

The core thesis—that a platform forfeits intermediary immunity the instant it “dynamically alters, processes, or actively sanitizes” user data—is a **contestable, largely aspirational reading** of Section 230 doctrine, not settled law, and USMCA Chapter 19 does essentially nothing to advance it for a private litigant. The strongest doctrinal footing for the thesis is the *Roommates.com* “material contribution to illegality” line and the Third Circuit’s 2024 *Anderson v. TikTok* holding that algorithmic recommendation is the platform’s “own first-party speech.” But the dominant line of authority (*Zeran*, *Jones v. Dirty World*, *Force v. Facebook*) treats curation, filtering, sorting, and even algorithmic arrangement as protected editorial functions squarely within Section 230, and *Roommates* itself protects “neutral tools.” The USMCA dimension is weaker still: the treaty is non-self-executing, creates no private right of action, and Article 19.17 by design does not require the U.S. to alter Section 230. Article 19.16’s source-code rule is a shield against forced disclosure as a condition of market access, not a substantive liability shield; and Article 32.1’s public-morals exception is a state-to-state defense, not a weapon a private plaintiff can wield against a platform’s data architecture.

TL;DR

- **The thesis is defensible but weak as stated.** “Dynamic alteration/processing/sanitizing” of user data does not, under prevailing law, strip Section 230 immunity; immunity is lost only where the platform *materially contributes to the unlawfulness* of content (the *Roommates* standard) or where the harm flows from the platform’s *own* conduct/speech (the *Anderson v. TikTok* theory). Ordinary moderation, curation, and algorithmic sorting remain protected editorial functions.
- **USMCA cannot be invoked by a private individual against a private platform.** It is non-self-executing (USMCA Implementation Act §102, 19 U.S.C. §4512), confers standing to challenge inconsistent measures only on the United States, and Article 19.17 expressly need not change U.S. law; it constrains governments, not private defendants.
- **The most potent lever for the thesis is *Anderson v. TikTok* post-*Moody*, but it cuts both ways:** treating algorithmic curation as the platform’s “expressive product” helps characterize the platform as an “actor,” yet the same *Moody v. NetChoice* reasoning simultaneously arms platforms with First Amendment protection for that curation.

Accurate Treaty-Text Mapping

Article 19.16 (Source Code) — verbatim

1. No Party shall require the transfer of, or access to, a source code of software owned by a person of another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory. international

↗

2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that

source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure. [international](#)

↗

Footnote 6 preserves trade-secret status of any code disclosed under paragraph 2. “Algorithm” is defined in Article 19.1 as “a defined sequence of steps, taken to solve a problem or obtain a result.” [international](#)

↗

Two exceptions/limits are textually critical: (a) the paragraph-1 prohibition bites only on demands made “as a condition for the import, distribution, sale or use” of software owned by “a person of another Party”—i.e., market-access conditions targeting foreign-owned code; and (b) paragraph 2 preserves regulatory-body and judicial access in a *specific* investigation/enforcement/judicial proceeding.

Scholarly interpretation is sharply split on whether 19.16 is a “shield” for opaque design:

- **Skeptical/critical reading (Kristina Irion, IViR/University of Amsterdam).** In “Algorithms Off-limits? If digital trade law restricts access to source code of software,” *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (FAccT ‘22), June 2022, doi:10.1145/3531146.3533212, Irion argues that “the clause on software source code is a double-edged sword that can conflict with the regulatory governance of digital technologies and in particular with algorithmic accountability. In spite of exceptions tailored to ensure that certain regulatory and judicial needs can be met, the trade law clause nevertheless curtails a government’s margin of discretion.” Crucially, she reads paragraph 2 as authorizing only “qualified transparency”—government access in *specific* investigations—so that generally-applicable, ex-ante mandates fall outside the safe zone: “Legislation that mandates conformity assessments, certification schemes or standardized APIs would be inconsistent with the protection of software source code inside trade law,” [ACM Digital Library](#)

↗

and rules enabling “public scrutiny by academics, media, critical engineers and civil actors would not be recognized under such a trade law clause.” [ACM Digital Library](#)

↗

This is the strongest support for the “shield for opaque/defensive system design” reading.

- **Counter-reading (Center for Data Innovation, 2018; industry groups).** Article 19.16 forbids only protectionist misuse of transparency demands. As the Center for Data Innovation put it, “the agreement would still allow parties to enact algorithmic transparency mandates for all firms, both foreign and domestic, [while] this provision prohibits them using algorithmic transparency as a protectionist measure.” [Center for Data Innovation](#)

↗

On this view, non-discriminatory, generally-applicable algorithmic-accountability laws remain permissible; CIGI similarly reads paragraph 2 as recognizing “that a regulatory body or judicial authority may need to scrutinize what an algorithm is doing.” [Centre for International Governance Innovation](#)

↗

The honest assessment: **the “shield” argument is real but limited.** 19.16 does not immunize a platform from liability; it constrains what disclosure a *government* can compel as a condition of market access. It does not, by its terms, prevent a court in litigation (paragraph 2) or a non-discriminatory transparency statute (the counter-reading) from reaching an algorithm. Its defensive value for opaque design is contested, not established.

Article 19.17 (Interactive Computer Services) — verbatim operative text

1. The Parties recognize the importance of the promotion of interactive computer services... as vital to the growth of digital trade. [international](#)

↗

2. To that end, other than as provided in paragraph 4, no Party shall adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created, or developed the information.

international

↗

3. No Party shall impose liability on a supplier or user of an interactive computer service on account of: (a) any action voluntarily taken in good faith by the supplier or user to restrict access to or availability of material... that the supplier or user considers to be harmful or objectionable; or (b) any action taken to enable or make available the technical means that enable an information content provider or other persons to restrict access to material that it considers to be harmful or objectionable. international

↗

4. Nothing in this Article shall: (a) apply to any measure of a Party pertaining to intellectual property...; or (b) be construed to enlarge or diminish a Party's ability to protect or enforce an intellectual property right; or (c) be construed to prevent: (i) a Party from enforcing any criminal law, or (ii) a supplier or user of an interactive computer service from complying with a specific, lawful order of a law enforcement authority.

5. This Article is subject to Annex 19-A. international

↗

Definitions (Art. 19.1): "**interactive computer service** means a system or service that provides or enables electronic access by multiple users to a computer server"; "**information content provider** means a person or entity that creates or develops, in whole or in part, information provided through the Internet or another interactive computer service." international

↗

Footnote 7 (attached to para. 2): "For greater certainty, a Party may comply with this Article through its laws, regulations, or application of existing legal doctrines as applied through judicial decisions." United States Trade Representative

↗

Footnote 8 (attached to 4(c)(ii)): "The Parties understand that measures referenced in paragraph 4(c)(ii) shall be not inconsistent with paragraph 2 in situations where paragraph 2 is applicable." Eric Goldman Blog

↗

Mirror-and-diverge from Section 230:

- Para. 2 tracks 47 U.S.C. §230(c)(1) ("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")
Socialmedialawbulletin
↗
and imports the §230(f)(3) "creation or development... in whole or in part" carve-out verbatim in substance.
- Para. 3 tracks §230(c)(2) (the "Good Samaritan" sword), though it uses "harmful or objectionable" rather than §230(c)(2)(A)'s longer list ("obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable").
- Para. 4 replicates §230(e)'s carve-outs for intellectual property (§230(e)(2)) and federal criminal law (§230(e)(1)).
- **Key divergences:** USMCA uses "supplier" not "provider"; drops §230's ambiguous "access software provider" language; and, most importantly, footnote 7 makes clear a Party may comply through *existing* doctrines/judicial decisions. Eric Goldman, writing at the Technology & Marketing Law Blog on October 3, 2018 ("Good News! USMCA (a/k/a NAFTA 2.0) Embraces Section 230-Like Internet Immunity"), observed: "I believe this is the first time any international treaty or free trade agreement has affirmatively embraced Section 230-like immunity."

- **Annex 19-A** delays application to Mexico for three years, presumes Mexico's Ley Federal de Telecomunicaciones (Arts. 145–146) consistent, and—decisively—subjects Article 19.17 to Article 32.1's public-morals exception, expressly citing FOSTA-SESTA (Public Law 115-164) as an example of a “measure necessary to protect public morals.”

The express non-alteration point: The USMCA Statement of Administrative Action and Implementation Act confirm that no change to §230 was required; Ambassador Lighthizer testified the language was included to make sure there were “no problems” [Disruptive Competition Project](#)

↗

with future Congressional action on §230. Article 19.17 codifies the *status quo*; it does not raise or lower the domestic bar.

Article 32.1 (General Exceptions / Public Morals)

Article 32.1.2 incorporates GATS Article XIV (including XIV(a), “necessary to protect public morals or to maintain public order”) into Chapter 19 *mutatis mutandis*; Article 32.1.1 incorporates GATT Article XX. Annex 19-A expressly confirms 19.17 is subject to this exception. [Global Affairs Canada](#)

↗

WTO interpretation of “public morals”:

- *US–Gambling* (Panel/AB, 2004–05): “public morals” denotes “standards of right and wrong conduct maintained by or on behalf of a community or nation,” and members enjoy “some scope to define and apply for themselves” these concepts. But the U.S. measures, though provisionally justified under XIV(a), *failed the chapeau* (arbitrary/unjustifiable discrimination) because of inconsistent treatment of domestic remote gambling.
- *EC–Seal Products* (AB, 2014): reaffirmed the *US–Gambling* definition and found the EU seal regime “provisionally necessary to protect public morals” under GATT XX(a), but again *not justified under the chapeau*.

Realistic assessment for leveraging against corporate data-tracking: Weak, and here is the skeptical view stated plainly. First, Article 32.1 is a **defense a state invokes to justify its own trade-restrictive measure**, not a cause of action; it presupposes a government has *already enacted* a measure regulating data-tracking. Second, the pattern in *US–Gambling* and *EC–Seal Products* is that even measures that clear the “public morals” hurdle repeatedly die at the chapeau if they discriminate. Third, no WTO adjudicator has ever addressed data-tracking architecture as a “public morals” matter; treating surveillance-advertising design as a morality question would be a novel extension with no precedent. It could *defend* a hypothetical U.S. data-privacy statute against a trade challenge; it does nothing to *create* platform liability.

The Platform-as-Actor Thesis: Steelman

The doctrinal engine is the statutory word “develop.” Section 230(f)(3) denies immunity to an entity “responsible, in whole or in part, for the creation or development of information.” [FindLaw](#)

↗

The thesis rides on an expansive reading of “development.”

1. **Fair Housing Council v. Roommates.com (9th Cir. 2008, en banc)** is the anchor. Chief Judge Kozinski held that by “requiring subscribers to provide [discriminatory preference] information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of the information.” [Wikipedia](#)

↗

The court defined “development” as “materially contributing to [content’s] alleged unlawfulness.” [Harvard](#)

This is the “co-developer” theory: a platform that shapes, structures, or compels the offending content transforms from host to information content provider. The steelman: a system that *dynamically alters or sanitizes* user data is, functionally, structuring the informational output—arguably “developing” it.

2. **Anderson v. TikTok, Inc., 116 F.4th 180 (3d Cir. 2024) (No. 22-3061, decided Aug. 27, 2024; panel opinion by Shwartz, J.)** is the thesis’s strongest modern authority. The panel held that TikTok’s “For You Page” algorithm “amalgamat[es] third-party videos” into “an expressive product” that is “TikTok’s own first-party speech,” so that “§230 does not bar Anderson’s claims.” The reasoning: because *Moody* deemed algorithmic curation the platform’s protected First Amendment expression, that same curation is the platform’s *own* speech—and §230 never immunized a platform’s own speech. This is precisely the “platform-as-actor” move: active curation converts the platform into a speaker/actor answerable for the output. (Note the limiting footnote: had Nylah found the video “through TikTok’s search function, rather than through her FYP, then TikTok may be viewed more like a repository of third-party content.”) The Third Circuit denied rehearing on October 23, 2024 (mandate issued Oct. 31, 2024); TikTok, through Paul Clement, obtained a cert-filing extension to February 20, 2025 (Application No. 24A681) but ultimately did not file a certiorari petition, leaving the panel opinion as binding Third Circuit precedent.
3. **The dissent/concurrence tradition feeding the thesis.** Judge Matey’s partial dissent in *Anderson* urged that §230’s scope is narrower than lower courts have held. Chief Judge Katzmman’s dissent in **Force v. Facebook (2d Cir. 2019)** argued §230 “bars lawsuits seeking to hold a service provider liable for its exercise of a publisher’s *traditional editorial functions*”—but recommendation algorithms that convey the platform’s own message exceed that, warning that “providers designed their algorithms to drive users toward content... nudging susceptible souls ever further down dark paths.” [Wikipedia](#)
- Justice Thomas** cited Katzmman approvingly in his *Malwarebytes* cert-denial statement and renewed the critique in *Doe ex rel. Roe v. Snap, Inc.*, 144 S. Ct. 2493 (2024) (Thomas, J., dissenting from denial of certiorari), observing that “in the platforms’ world, they are fully responsible for their websites when it results in constitutional protections, but the moment that responsibility could lead to liability, they can disclaim any obligations,” and urging that “the Court should consider if this state of affairs is what §230 demands.” In *Gonzalez v. Google* (9th Cir. below), Judge Gould’s partial dissent adopted Katzmman’s view.
4. **The AI-transformation extension.** Where a platform’s system does not merely arrange but *generates or materially transforms* the informational output (e.g., an LLM synthesizing a response, or a system that “sanitizes”/rewrites user input), the “creation or development... in whole or in part” language is at its most textually available, because the platform is authoring part of the output. This is the frontier where the thesis is strongest in principle and least tested in fact.

The Platform-as-Actor Thesis: Hostile Stress-Test

Here is where the thesis is weakest, named explicitly.

1. **Zeran v. AOL (4th Cir. 1997)** is the foundational counterweight and remains the majority rule. It holds §230 “creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user,” and—critically—“lawsuits seeking to hold a service provider liable for its exercise of a publisher’s *traditional editorial functions*—such as deciding whether to publish, withdraw, postpone or alter content—are barred.” *Altering* content is the paradigmatic protected editorial function. The thesis’s claim that “altering, processing, or sanitizing” strips immunity runs headlong into *Zeran*: those are exactly the acts §230 protects. *Zeran* also rejected notice-based/distributor liability, foreclosing the argument that a platform’s *knowledge* of harmful content converts it into an actor.

2. **“Neutral tools” survive Roommates.** The en banc court was emphatic: “providing neutral tools to carry out what may be unlawful or illicit searches does not amount to ‘development.’” [Ninth Circuit Court](#)
 ↗
 A search engine returning results for “white roommate” “has not contributed to any alleged unlawfulness.” Immunity is lost only by “materially contributing to [the] *unlawfulness*”—not by processing, sorting, or arranging per se. Because most dynamic data processing is content-neutral, *Roommates* protects it. Judge McKeown’s partial dissent warned the majority already went too far and “threatens to chill the robust development of the Internet.” [Wikipedia](#)
 ↗
3. **Jones v. Dirty World (6th Cir. 2014)** applied *Roommates*’ material-contribution test and held that a site that *selected which user submissions to publish and added its own satirical commentary* still did not “materially contribute” to defamatory content—cautioning that a broad reading of “development” “would defeat the purposes of the CDA and swallow the core immunity.” [Jaburg Wilk](#)
 ↗
 This directly rebuts the notion that editorial selection or annotation equals “development.”
4. **Force v. Facebook (2d Cir. 2019, majority)** squarely rejected the algorithm-as-development theory: there is “no basis... for concluding that an interactive computer service is not the ‘publisher’ of third-party information when it uses tools such as algorithms that are designed to match that information with a consumer’s interests,” because “arranging and distributing third-party information inherently forms ‘connections’ and ‘matches.’” The majority further held that Facebook “acquiring certain information from users” (names, phone numbers, emails) did *not* render it a “developer”—a [Eric Goldman Blog](#)
 ↗
 direct rebuttal to the “processing user data = actor” claim. TikTok’s own Supreme Court cert-extension application (Application No. 24A681, filed Jan. 6, 2025) conceded that the Third Circuit’s reading conflicts with the “Fifth, Sixth, Eighth, Ninth, Tenth, and D.C. Circuits,” which the *Anderson* panel had “dismissed... as having ‘pre-dated NetChoice.’” In other words, the weight of circuit authority aligns with *Force*, not *Anderson*.
5. **Gonzalez v. Google (2023) did not adopt the thesis.** The Supreme Court took the case to decide whether §230 covers algorithmic recommendations and then *punted*, resolving the companion *Twitter v. Taamneh* on the merits (no aiding-and-abetting) and remanding *Gonzalez* per curiam, “declin[ing] to address the application of §230.” Result: **the pre-existing broad-immunity status quo is unchanged**, and the platform-as-actor theory got no Supreme Court endorsement.
6. **The Moody boomerang cuts against the thesis as much as for it.** *Moody v. NetChoice* (2024) held that platforms’ “selection, ordering, and ranking of third-party content is expressive and thus protected by the First Amendment”—that [www.hlc.com](#)
 ↗
 “presenting a curated and ‘edited compilation of [third-party] speech’ is itself protected speech.” *Anderson* leveraged this to say curation is the platform’s *own* speech (helping the “actor” label). But the same holding hands platforms a **constitutional shield**: if curation is protected expression, then statutes or tort theories that penalize curation face First Amendment scrutiny. As Techdirt argued in “The Third Circuit’s Section 230 Decision In *Anderson v. TikTok Is Pure Poppyclock*” (Sept. 3, 2024), *Anderson*’s logic proves too much: “a platform’s decision to host a third party’s speech at all is also First Amendment-protected expression. By the Third Circuit’s logic, then, such hosting decisions, too, are a platform’s ‘own first-party speech’ unprotected by Section 230”—which cannot be right. Justice Alito’s concurrence called the majority’s expressive-curation discussion “nonbinding dicta,” and *Moody* itself expressly reserved whether *non-expressive* algorithmic sorting (algorithms “respond[ing] solely to how users act online”) [www.hlc.com](#)
 ↗
 receives the same treatment. The doctrinal terrain is unstable, not settled in the thesis’s favor.

Bottom line on the thesis: As a description of *current majority law*, “dynamic alteration/processing/sanitizing strips immunity” is **false**. As a *live minority position with momentum* (Anderson, Katzmman, Thomas, Matey, Gould), it is real but confined to one circuit, in tension with a First Amendment counter-shield, and unratified by the Supreme Court. The precise, defensible version of the thesis is narrower: *immunity is lost only where the platform’s own conduct or expression—not the third-party content—is the source of the alleged harm, or where the platform materially contributes to the content’s unlawfulness*.

What This Doctrine Can and Cannot Do

USMCA cannot help a private litigant sue a platform. This must be stated without hedging:

1. **Non-self-executing / U.S. law prevails.** USMCA Implementation Act §102 (19 U.S.C. §4512) provides that no USMCA provision inconsistent with U.S. law has effect, and that U.S. law prevails in any conflict. [GovInfo](#)
↗
The Statement of Administrative Action confirms “no existing federal law... will be required to implement the new international obligations.” [United States Senate Committee on Finance](#)
↗
The treaty does not supply a rule of decision in domestic litigation.
2. **No private right of action.** §102(c) bars any person other than the United States from asserting a “cause of action or defense” under the USMCA, or from challenging any government action as inconsistent with the USMCA. Only the United States may bring such an action, and only against governmental measures. A private plaintiff cannot cite Article 19.17 (or 19.16, or 32.1) against a private platform, and a platform cannot cite them as a defense in a private suit.
3. **State-to-state, not private, obligations.** Chapter 19 disciplines what *governments* may enact. Article 19.17 constrains a Party from *adopting measures* that treat an ICS as a content provider; it says nothing a private tort plaintiff can invoke. This is confirmed in practice: in Canadian litigation (*Giustra v. Twitter*; the Google/Quebec defamation matter), courts rejected arguments that CUSMA/USMCA Article 19.17 imports §230-style immunity into domestic private law.
4. **Article 19.17 expressly does not require changing §230.** The provision codifies existing U.S. law; footnote 7 permits compliance “through... existing legal doctrines as applied through judicial decisions.” [United States Trade Representative](#)
↗
It neither expands nor contracts a private plaintiff’s ability to defeat immunity.

What the doctrine can do: frame policy debate; inform how a treaty-conscious court might construe ambiguous domestic law consistently with international obligations (the *Charming Betsy* canon, a weak interpretive nudge); and constrain *future U.S. or state legislation* that would strip platform immunity (a government measure treating ICSs as content providers could, in theory, be challenged by *Canada or Mexico* as USMCA-inconsistent—but again, only state-to-state).

What Article 19.16 can and cannot do: it can block a *government* from conditioning market access on source-code/algorithm disclosure and constrains the design of ex-ante transparency mandates (Irion’s concern); it cannot shield a platform from producing code under paragraph 2 in actual litigation or a regulatory investigation, and it creates no liability immunity.

Historical/Structural Parallel (Framing Device — Analogy, Not Authority)

The following is offered as an intellectual lens, clearly labeled as analogy and carrying no legal weight.

Nineteenth-century American law confronted a structurally similar problem: how to allocate liability and access rights over privately owned infrastructure that carried a shared public resource. Two bodies of doctrine are instructive:

- **The Mill Acts and *Head v. Amoskeag Mfg. Co.* (113 U.S. 9, 1885).** States authorized mill owners to dam non-navigable streams and flood upstream neighbors' land, provided they paid damages. [Wikipedia](#)

↗

The Supreme Court upheld New Hampshire's General Mill Act as "a just and reasonable exercise of the power of the legislature... to regulate the use of the water power of running streams, which without some such regulation could not be beneficially used." [Justia](#)

↗

The analogy: the mill owner is a *private actor operating shared-resource infrastructure* whose "reasonable use" is tolerated but *conditioned*—liability attaches when its operations impose external harm (flooding), and the sovereign retains regulatory power over the flow. A platform that dams and redirects the "data flow" might, by analogy, be seen as owing compensation/liability for downstream harm—but note the disanalogy the thesis must confront: the mill's liability was for *physical spillover onto others' property*, established by statute, not for the *content* of what flowed.

- **Common-carrier duties and riparian "reasonable use."** The common-carrier tradition (ferries, gristmills, stagecoaches—"common callings" with a "duty to serve" [Paul Daly](#)

↗

without discrimination) and riparian doctrine (a downstream owner's right to receive water "undiminished in flow and quality") [Wikipedia](#)

↗

both regulate actors who control a conduit of shared value. The modern debate over treating platforms as common carriers (Fordham Law Review, 2022; and Justice Thomas's *Biden v. Knight* concurrence) draws directly on this lineage. But the scholarship is candid that the analogy breaks precisely where the platform-as-actor thesis needs it most: as the Fordham analysis concludes, common-carrier treatment "would not address the underlying problem... because those platforms are not mere conduits; instead, they actively participate in the facilitation and amplification of user content." [Fordham Law Review](#)

↗

The very "activeness" that the platform-as-actor thesis invokes to *strip* immunity is the same quality that *defeats* the common-carrier (passive conduit) framing. The two theories pull in opposite directions.

The honest takeaway from the analogy: industrial-era doctrine shows the law has long conditioned the rights of private operators of shared-resource infrastructure and imposed liability for spillover harms. But it also shows that liability attached to *physical externalities* under *express legislative* schemes—not to the informational content carried, and not through judicial reinterpretation of an immunity statute. The analogy motivates the thesis; it does not authorize it.

Recommendations

1. **Reframe the thesis to the defensible core.** Do not assert that "alteration/processing/sanitizing" strips immunity—that contradicts *Zeran* and *Force*. Assert instead: *immunity is unavailable where (a) the platform materially contributes to the content's unlawfulness (Roommates), or (b) the alleged harm arises from the platform's own conduct or expressive product rather than the third-party content (Anderson)*. This survives hostile scrutiny.
2. **Stage the litigation theory by circuit and by function.** In the **Third Circuit**, *Anderson* is live precedent for algorithmic-recommendation-as-first-party-speech; build claims around *proactive, unprompted* algorithmic promotion (not search-responsive delivery, which *Anderson's* footnote protects). Elsewhere, expect

Force/Zeran to control; preserve the issue for Supreme Court review, which *Gonzalez* left open and which TikTok's own filings concede presents a circuit split.

3. **Target AI-generative/transformational conduct, not curation.** The “development... in whole or in part” text is strongest where the system *authors or materially rewrites* output. A system that “sanitizes”/transforms user input into new content is a better vehicle than one that merely ranks or filters.
4. **Drop USMCA as a source of private leverage entirely.** Do not plead or rely on Articles 19.16, 19.17, or 32.1 in private litigation against a platform; §102 of the Implementation Act forecloses it and it will invite dismissal of that theory. Use USMCA only as (a) policy framing, or (b) a constraint to anticipate if advocating *legislation* stripping immunity (which Canada/Mexico could challenge state-to-state).
5. **Watch the *Moody* remands and any circuit split.** Benchmarks that would change the analysis: (a) a circuit split ripening from *Anderson* that the Supreme Court agrees to resolve; (b) a Supreme Court merits ruling on §230's coverage of algorithmic recommendation; (c) a *Moody* remand decision clarifying whether *non-expressive* algorithmic sorting loses First Amendment protection (which would let plaintiffs pursue the “actor” theory *without* handing platforms a constitutional shield). Any of these would materially strengthen or sink the thesis.
6. **On Article 19.16, adopt Irion's framing but note its contested status.** If arguing that trade law entrenches algorithmic opacity, cite Irion (FAcCT 2022) for the “qualified transparency” critique, but concede the Center for Data Innovation counter-reading that non-discriminatory, generally-applicable transparency mandates remain permissible and that paragraph 2 preserves regulatory/judicial access.

Caveats

- **The thesis is novel/aspirational, not settled.** *Anderson v. TikTok* is a single-circuit outlier decided on contested First Amendment reasoning (EPIC called it “questionable First Amendment reasoning”; Techdirt called it “poppycock”); it diverges from the Fifth, Sixth, Eighth, Ninth, Tenth, and D.C. Circuits' pre-*Moody* §230 jurisprudence (as TikTok's own cert-extension application conceded). Do not present it as majority law.
- **The First Amendment tension is unresolved and double-edged.** *Moody*'s core holdings are, by Justice Alito's account and the majority's own framing, substantially dicta on a facial-challenge posture; the Court reserved the treatment of non-expressive algorithms. Relying on *Moody* to characterize platforms as “actors” simultaneously supplies them constitutional cover.
- **USMCA claims against private platforms will fail.** This is the single most important guardrail: any framing suggesting a private individual can invoke USMCA against a platform overstates the doctrine and is legally incorrect under §102 of the Implementation Act.
- **WTO “public morals” has never reached data architecture,** and even successful “public morals” measures have repeatedly failed the chapeau (*US–Gambling*, *EC–Seal Products*). Treating it as a lever against corporate data-tracking is speculative.
- **Source quality note:** case holdings herein are drawn from primary opinions (9th, 4th, 2d, 3d Circuits; Supreme Court) and official treaty/statutory text (USTR, Global Affairs Canada, Cornell LII, Congress.gov); commentary characterizations (Goldman, EPIC, Techdirt, Federalist Society, CRS) are identified as such. The Irion quotations were captured via the ACM full text and should be page-verified against the published PDF (FAcCT '22, pp. 1561–1570) before formal pin-citation.
- **The historical analogy is illustrative only** and carries no precedential force; it is included as an interpretive framing device at the reader's request, with its principal disanalogies named.