Statutory Framing, Constitutional Boundaries, and Technical Enforcement of Online Extremism: A Multi-Jurisdictional Analysis

Section 1: Comparative Alignment Matrix: Federal Statutory Baseline Versus Platform Governance

Federal statutory frameworks and private platform governance mechanisms operate from fundamentally divergent structural baselines. U.S. federal law establishes a bifurcated approach that separates international terrorism from domestic terrorism under 18 U.S.C. § 2331, applying distinct enforcement mechanisms, criminal penalties, and constitutional constraints to each category. In contrast, commercial digital platforms formulate terms of service, acceptable use policies, and violent extremism standards that operate globally, targeting conduct, association, and expressive radicalization dynamics prior to the commission of any criminal predicate act.

Legal / Policy Dimension	18 U.S.C. § 2331(1) & (5) (Federal Statutory Baseline)	28 C.F.R. § 0.85(l) (Federal Law Enforcement Operational Baseline)	Private Platform Governance (Google/YouTube, Meta, X Policies)	Operational and Conceptual Alignment
Intent & Coercive Purpose	Requires activities that appear intended to: (i) intimidate or coerce a civilian population; (ii) influence government policy by intimidation or coercion; or (iii) affect government conduct by mass destruction, assassination, or kidnapping.	Targets the unlawful use of force or violence committed to "intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives".	Prohibits content that promotes, facilitates, glorifies, or incites violence, ideological coercion, or intimidation, regardless of whether a formal state or political target is identified.	Platforms decouple intent from statutory evidentiary standards, evaluating expressive harms, radicalization pipelines, and perceived offline threats rather than formal criminal mens rea.
Physical Harm & Predicate Acts	Must involve "acts dangerous to human life" that constitute a violation of the criminal laws of	Encompasses the "unlawful use of force and violence against persons or property".	Extends beyond physical violence to encompass ideological manifestos, recruitment	Platforms apply a precautionary moderation threshold, intervening upstream at the

Legal / Policy Dimension	18 U.S.C. § 2331(1) & (5) (Federal Statutory Baseline)	28 C.F.R. § 0.85(l) (Federal Law Enforcement Operational Baseline)	Private Platform Governance (Google/YouTube, Meta, X Policies)	Operational and Conceptual Alignment
	the U.S. or any state (or that would be a criminal violation if committed within jurisdiction).		propaganda, financial solicitation, digital coordination, and glorification of past mass attacks.	expressive and preparatory phases, whereas statutes require an underlying criminal predicate act dangerous to human life.
Public Safety & Infrastructure	Explicitly defines statutory domestic terrorism via methods including mass destruction, assassination, or kidnapping occurring primarily within U.S. territorial jurisdiction.	Focuses on disruptions to public order, state functions, and civilian safety resulting from violent or forcible acts.	Restricts attacks on critical physical or digital infrastructure, cyber-attacks, doxxing of public officials, coordinated mass harassment, and distribution of weapon blueprints or tactical execution materials.	Both domains target threats to critical infrastructure, but platform enforcement intervenes at the information-distribution layer (e.g., instructional material) rather than post-incident operational execution.
Entity Designation & List Authority	Differentiates between Foreign Terrorist Organizations (FTOs designated under INA § 219 / 8 U.S.C. § 1189) and domestic actors; contains no statutory designation mechanism or domestic terrorist organization list.	Directs the FBI to investigate domestic and international terrorism under enterprise rules without maintaining a formal, published domestic group blacklist.	Maintains proprietary lists of Dangerous Individuals and Organizations (DIO) and Violent Extremist Organizations (VEO), encompassing foreign entities, transnational movements, and domestic extremist groups.	Major divergence: Platforms bridge the domestic/international statutory divide by privately designating domestic entities (e.g., white supremacist groups, violent sovereign citizen factions) that the state is constitutionally barred from blacklisting.
Material Support & Propagation	Criminalizes knowingly providing material	Authorizes investigative and intelligence	Prohibits any digital presence, account creation,	Corporate policies operate as private material support

Legal / Policy Dimension	18 U.S.C. § 2331(1) & (5) (Federal Statutory Baseline)	28 C.F.R. § 0.85(l) (Federal Law Enforcement Operational Baseline)	Private Platform Governance (Google/YouTube, Meta, X Policies)	Operational and Conceptual Alignment
	support or resources to designated FTOs under 18 U.S.C. § 2339B; lacks a general domestic material support analogue absent an independent predicate offense.	collection tools (subject to Attorney General Guidelines) against enterprises planning or committing federal crimes.	content monetization, link-sharing, or amplification of designated entities, their manifestos, or affiliated media production arms.	prohibitions, treating account access, hosting, and algorithmic distribution as impermissible digital facilitation of extremist groups.

The statutory architecture of 18 U.S.C. § 2331 establishes a functional distinction between international terrorism under subsection (1) and domestic terrorism under subsection (5). While both definitions share identical core prongs regarding the appearance of intent—intimidating civilians, influencing policy, or affecting government conduct through mass destruction, assassination, or kidnapping—they bifurcate on territorial jurisdiction and executive designation authorities.

Under international terrorism provisions, the executive branch leverages designation authority under Section 219 of the Immigration and Nationality Act (8 U.S.C. § 1189) and Executive Order 13224 to issue binding Foreign Terrorist Organization (FTO) and Specially Designated Global Terrorist (SDGT) lists. These designations trigger strict liability criminal material support prohibitions under 18 U.S.C. § 2339B, which withstand constitutional challenge because foreign entities operating abroad do not possess First Amendment rights (*Holder v. Humanitarian Law Project*, 2010).

Conversely, domestic terrorism under 18 U.S.C. § 2331(5) functions primarily as an investigatory classification, a sentencing enhancement factor under U.S.S.G. § 3A1.4, or a jurisdictional threshold for specific investigative authorities under the Attorney General's Guidelines for Domestic FBI Operations. It does not create a standalone substantive federal crime for purely domestic acts absent an independent federal violent offense, such as acts involving weapons of mass destruction under 18 U.S.C. § 2332a or acts of terrorism transcending national boundaries under 18 U.S.C. § 2332b.

The operational definition under 28 C.F.R. § 0.85(l) governs the FBI’s primary investigative mandate across all terrorism matters within U.S. jurisdiction. It focuses on the unlawful use of force or violence against persons or property to intimidate or coerce a government or civilian population for political or social goals.

Commercial platforms construct policies that bypass these statutory jurisdictional limitations. Corporate violent extremism policies merge foreign and domestic entities into unified operational frameworks, such as Meta’s Dangerous Organizations and Individuals (DOI) framework and Google/YouTube’s Violent Extremist Organizations (VEO) policy. Platforms execute a tiered enforcement model:

- Tier 1 entities (FTOs, SDGTs, and recognized mass-casualty violent extremist groups) face total deplatforming, encompassing praise, representation, manifestos, iconography, and ideological propaganda.

- Tier 2 and Tier 3 entities (unorganized violent groups, violent non-state actors, and hate-based extremist networks) face functional restrictions on monetization, recruitment, and targeted distribution.

By decoupling enforcement from statutory criminal predicates, platforms penalize pre-operational speech, ideological propaganda, aesthetic subcultures (e.g., terrorwave imagery), and extremist manifestos. Platforms enforce content bans based on qualitative assessments of potential offline harm, operating proactive algorithmic removals and hash-database matching via the Global Internet Forum to Counter Terrorism (GIFCT) where statutory law requires an underlying criminal act dangerous to human life.

Section 2: Constitutional Divergence and Platform Editorial Discretion

The United States Constitution establishes an asymmetric legal environment wherein the sovereign state and private platforms operate under fundamentally different speech governance frameworks. Under the State Action Doctrine articulated in the *Civil Rights Cases* (1883) and *Lugar v. Edmondson Oil Co.* (1982), the First Amendment operates strictly as a negative check on governmental power, rather than a restriction on private commercial entities. When the Department of Justice, the FBI, or state law enforcement agencies seek to restrict, penalize, or censor speech associated with domestic political extremism, their actions are constrained by strict scrutiny and the incitement test articulated in *Brandenburg v. Ohio* (1969).

Under *Brandenburg*, the state cannot proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action. This constitutional standard protects a wide array of domestic extremist rhetoric. Abstract praise for historical acts of political violence, generalized calls for revolution, white supremacist ideology, eco-extremist philosophy, and anti-government militia doctrine remain constitutionally protected speech. The Supreme Court reinforced this high evidentiary threshold in *Counterman v. Colorado* (2023) and *Virginia v. Black* (2003), requiring that to prosecute true threats, the state must establish that the speaker acted with at least a subjective mental state of recklessness regarding the threatening nature of their communication, or acted with a specific intent to intimidate.

Consequently, the U.S. government cannot establish a formal domestic terrorist organization list without violating First Amendment protections concerning freedom of association (*NAACP v. Alabama*, 1958) and viewpoint-based discrimination (*R.A.V. v. City of St. Paul*, 1992). Any statutory attempt by the federal government to prohibit membership in, or peaceful material support to, a domestic political organization would trigger strict scrutiny, failing the requirement of narrow tailoring unless the state can prove an individual's specific intent to further the group's illegal, violent aims (*Scales v. United States*, 1961).

While the First Amendment restricts state intervention against extremist advocacy, it protects the editorial discretion of private platforms. In *Moody v. NetChoice, LLC* (2024), the Supreme Court confirmed that major social media platforms and interactive digital services engage in expressive activity protected by the First Amendment when curating, organizing, ranking, and moderating third-party content. The *Moody* Court established that compiling and curating third-party speech—deciding what content to include, exclude, prioritize, or demote—constitutes editorial judgment analogous to the constitutionally protected choices made by traditional newspapers, parade organizers, and utility newsletter publishers (*Miami Herald Publishing Co. v. Tornillo*, 1974; *Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston*, 1995;

Pacific Gas & Electric Co. v. Public Utilities Commission, 1986).
The Court rejected the argument advanced by Florida and Texas that large social media networks function as common carriers stripped of First Amendment rights. The majority opinion clarified that state regulations compelling platforms to host speech contrary to their internal community standards impermissibly alter the expressive compilation of the platform.
Simultaneously, statutory platform governance in the United States is anchored by Section 230 of the Communications Decency Act of 1996 (47 U.S.C. § 230). Under 47 U.S.C. § 230(c)(1), interactive computer services are shielded from being treated as the publisher or speaker of information provided by third-party content creators, neutralizing common-law publisher liability for torts, defamation, or civil harms stemming from hosted user content. Complementing this protection, 47 U.S.C. § 230(c)(2)(A) immunizes platforms from civil liability for voluntary actions taken in good faith to restrict access to, or availability of, material considered obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.
This statutory and constitutional structure allows private platforms to enforce proactive harm thresholds on domestic political rhetoric that the state is constitutionally forbidden to censor. Platforms routinely deplatform domestic extremist groups, remove sovereign citizen manifestos, suppress election-denial movements that carry latent threats of violence, and restrict hate speech without demonstrating imminent lawless action under *Brandenburg*. While the state must prove an act dangerous to human life and establish specific intent to coerce under 18 U.S.C. § 2331(5), private platforms take proactive action based on corporate terms of service and internal risk management policies.

Section 3: Global Regulatory Conflict Matrix: U.S. Common-Carrier Statutes Versus International Co-Regulation

Interactive online platforms face conflicting regulatory mandates across global jurisdictions. In the United States, state statutes attempt to enforce common-carrier obligations on viewpoint-based speech, while federal reform proposals aim to condition Section 230 immunity on content neutrality, child safety metrics, or algorithmic transparency. Conversely, the European Union has implemented a co-regulatory liability framework through the Digital Services Act (DSA) and the Terrorist Content Online (TCO) Regulation, imposing systemic risk mitigation mandates and strict turnaround times for removing illegal content.

Governance Parameter	U.S. State Common-Carrier Laws (Texas HB 20, Florida SB 7072)	U.S. Federal Section 230 Reform Proposals (e.g., EARN IT, Platform Accountability)	EU Digital Services Act (DSA - Reg. 2022/2065) & TCO (Reg. 2021/784)
Core Regulatory Philosophy	Common-carrier paradigm; treats large social networks as public forums; restricts viewpoint discrimination and content suppression.	Conditional immunity; ties Section 230 liability shields to procedural due process, child safety metrics, or removal of federal illegal content.	Co-regulatory risk governance; imposes systemic risk assessment, transparency, and administrative liability on platform operations.
Treatment of Political	Prohibits removing,	Seeks to narrow §	Mandates the

Governance Parameter	U.S. State Common-Carrier Laws (Texas HB 20, Florida SB 7072)	U.S. Federal Section 230 Reform Proposals (e.g., EARN IT, Platform Accountability)	EU Digital Services Act (DSA - Reg. 2022/2065) & TCO (Reg. 2021/784)
/ Extremist Speech	deplatforming, demonetizing, or deprioritizing user content based on viewpoint or geographic origin within the state.	230(c)(2)(A) protections to prevent the suppression of lawful political discourse or strip algorithmic promotion protections.	mitigation of systemic risks to civic discourse, public security, and fundamental rights under Articles 34 and 35.
Mandatory Content Removal Thresholds	Narrow: Limits mandatory removals to strictly unlawful speech (e.g., child sexual abuse material, direct illegal incitement, true threats).	Variable: Proposes carving out federal civil causes of action, anti-terrorism statutes, and specific torts from immunity protections.	Strict: DSA Articles 16 & 34 require proactive notice-and-action; TCO Art. 3 mandates removal of flagged terrorist content within 1 hour.
Enforcement Mechanisms & Penalties	Private rights of action by users and state Attorney General enforcement; civil statutory damages per individual violation.	Revocation of Section 230 statutory immunity, exposing platforms to direct civil publisher liability in state and federal courts.	European Commission and national Digital Services Coordinators; administrative fines up to 6% of global annual turnover (DSA Art. 52).
Extraterritorial & Operational Reach	Enforceable against actions affecting residents within state territorial boundaries (Texas/Florida).	Enforceable nationwide across all interactive computer services operating within U.S. federal jurisdiction.	Enforceable across the European Single Market for all designated Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs).

Platforms navigate competing legal risks across these jurisdictions. In the United States, removing lawful but incendiary domestic political speech creates exposure to state-level statutory penalties under Texas HB 20 or Florida SB 7072 (pending final post-*Moody* lower-court applications). In the European Union, failing to aggressively mitigate systemic risks associated with the spread of extremist or illegal content exposes Very Large Online Platforms (VLOPs) to administrative fines of up to 6% of their global annual turnover under DSA Articles 34, 35, and 52, alongside structural penalties under the TCO Regulation for failing to execute 1-hour removal orders.

To reconcile these opposing mandates, platforms implement operational and legal firewalls:

1. **Bifurcation of Terms of Service**: Platforms establish distinct corporate contracting entities for different jurisdictions. Users within the European Economic Area (EEA) contract with European subsidiaries (e.g., Google Ireland Limited, Meta Platforms Ireland Limited), operating under terms governed by Irish or local member-state law and structured around DSA-compliant notice-and-action frameworks. U.S. users contract with domestic parent entities (Google LLC, Meta Platforms, Inc.) governed by Delaware or California law and centered on broad Section 230(c)(2)(A) reservations of editorial discretion.

2. **Decoupled Algorithmic Pipelines**: Rather than deploying a uniform global recommender architecture, platforms apply regional filtering and ranking parameters. Content circulating within the EEA is routed through automated risk-scoring filters calibrated to identify hate speech, disinformation, and violent extremism under DSA Articles 34 and 35. In the U.S., platforms adjust recommender systems to balance brand safety and civil liability against legal and political scrutiny concerning algorithmic viewpoint suppression.
3. **Jurisdiction-Specific Content Geoblocking**: When a competent national authority in the EU issues a formal removal order, or when an EU DSA audit identifies high-risk systemic harms, platforms implement geo-fenced withholding. The underlying content remains accessible to users resolving from U.S. IP addresses but returns an HTTP 451 ("Unavailable For Legal Reasons") status code or localized content warning to users accessing the service from within the EEA.

Section 4: Technical Implementation, Evasion Mechanics, and Detection Infrastructure

Executing jurisdictionally differentiated content moderation requires platforms to maintain reliable technical attribution of user physical location. However, basic IP-based geolocation is often undermined by network anonymization techniques, requiring platforms to deploy multi-layered detection stacks across the transport, client, and application layers.

Network Anonymization Mechanics and Geo-Fencing Degradation

Threat actors, extremist networks, and general users bypass geographic restrictions using three primary network evasion models:

1. **Commercial Virtual Private Networks (VPNs)**: VPN clients establish an encrypted tunnel using protocols such as OpenVPN, WireGuard, or IPsec from the client device to an egress server in a target jurisdiction. The platform's edge server sees the public IPv4 or IPv6 address of the VPN egress node rather than the client's residential IP. This masks client origin, but the traffic typically emerges from Autonomous System Numbers (ASNs) registered to commercial data centers and hosting providers (e.g., DigitalOcean, AWS, OVH, M247) rather than residential Internet Service Providers (ISPs).
2. **Residential Proxy Networks**: To evade data-center IP blacklists, threat actors route traffic through residential proxy networks (e.g., Bright Data, Oxylabs) or peer-to-peer networks (such as proxy-ware SDKs embedded in mobile applications). Traffic from the client is relayed through consumer broadband or mobile connections, giving the egress traffic an ASN classification belonging to consumer ISPs (e.g., Comcast, Deutsche Telekom, AT&T), which bypasses static IP reputation blocklists.
3. **Smart DNS / DNS Redirection**: Smart DNS services alter DNS resolution paths without encrypting the entire transport stream. When a client queries a domain name subject to geo-fencing, the Smart DNS resolver returns the IP address of an intermediate transparent proxy server located in the desired jurisdiction for the authentication handshake, while media streams may resolve directly.

The Multi-Layered Technical Enforcement Stack

To enforce territorial compliance and prevent circumvention, platforms deploy an integrated,

defense-in-depth telemetry stack that operates across the network, client, and application layers:

Network and Transport-Layer Telemetry

- **Autonomous System Number (ASN) and Subnet Classification**: Ingress connections are evaluated against real-time IP intelligence feeds (e.g., MaxMind GeoIP2, IPinfo, Spur). IPs classified as commercial data centers, hosting providers, or known proxy endpoints face challenge screens (e.g., Cloudflare Turnstile, reCAPTCHA v3) or access restrictions for geo-sensitive material.
- **Anycast BGP Latency Triangulation**: Platforms deploy Anycast Border Gateway Protocol (BGP) routing across distributed Points of Presence (PoPs). By measuring the Round-Trip Time (RTT) of TCP SYN/ACK packets across multiple global ingress nodes, the platform establishes physical speed-of-light propagation bounds:t \ge \frac{2d}{c \cdot \frac{2}{3}} Where d represents physical distance and c is the speed of light in vacuum. If an IP address claims to be in Frankfurt, Germany, but exhibits an RTT baseline of 140 ms to the Frankfurt PoP and 12 ms to an Ashburn, Virginia PoP, the platform identifies proxy routing and overrides the claimed IP location.
- **Deep Packet Inspection (DPI) and TLS Fingerprinting**: Platforms inspect transport-layer packet headers. Using JA3/JA3S and JA4 fingerprinting algorithms, edge servers hash the parameters of the TLS ClientHello packet (including TLS version, accepted cipher suites, extensions, supported elliptic curves, and point formats). Proxy client runtimes (such as Shadowsocks, V2Ray, or automated Python scrapers) generate distinct TLS fingerprints compared to standard web browsers (e.g., Google Chrome on Windows/macOS), enabling edge proxies to drop connections or apply regional fallbacks regardless of the reported IP address.

Client-Side Telemetry and Hardware Probing

- **WebRTC ICE Candidate Enumeration**: Modern web browsers implement the WebRTC (Web Real-Time Communication) protocol for peer-to-peer media sessions. Platforms execute client-side JavaScript that initiates a WebRTC connection via Interactive Connectivity Establishment (ICE) using Session Traversal Utilities for NAT (STUN) servers. The STUN resolution extracts the true host network interfaces, exposing local private IPv4 addresses (e.g., 192.168.1.X, 10.X.X.X) and actual public IPv6/IPv4 endpoints directly assigned to the client's physical network card, bypassing client-level VPN tunnels that fail to route UDP or WebSockets traffic.
- **Wi-Fi BSSID and Ambient RF Triangulation**: On mobile applications (iOS/Android), platform SDKs query the local network subsystem to collect the Basic Service Set Identifiers (BSSIDs)—the MAC addresses of nearby Wi-Fi routers—alongside Received Signal Strength Indication (RSSI) metrics and Cell Tower Global Identity (CGI/eNodeB ID) metadata. These identifiers are checked against proprietary geolocation databases (e.g., Google Location Services, Skyhook). Ambient RF positioning provides physical location accuracy within meters, bypassing operating system IP-level VPN overrides.
- **HTML5 Geolocation and Native GPS Interfaces**: Platforms request hardware-level coordinates via the navigator.geolocation API on desktop browsers and Location Services subsystems on mobile devices. This data surfaces raw GPS NMEA sentences (latitude, longitude, altitude, horizontal dilution of precision), providing physical location attribution

independent of the transport-layer network pathway.

Behavioral, Clock, and Application-Layer Heuristics

- **System Clock and NTP Desynchronization**: Browsers execute JavaScript to measure the delta between the local system time (Date.now(), Intl.DateTimeFormat().resolvedOptions().timeZone) and the Network Time Protocol (NTP) timestamp returned in server HTTP response headers (Date:). An IP address resolving to Berlin (UTC+1/UTC+2) paired with a device system clock set to Austin, Texas (UTC-6) triggers an anomaly flag, signaling proxy mediation.
- **TCP/IP Stack Fingerprinting**: Operating systems configure TCP packet parameters differently. Platforms analyze the initial Time-to-Live (TTL) values, TCP Window Size, Maximum Segment Size (MSS), and TCP Options ordering. A connection presenting a Linux TCP packet profile matching a data-center proxy server, paired with a User-Agent header claiming to be an Apple Safari browser on iOS, triggers automated policy down-ranking.
- **Linguistic and Interface Interaction Profiles**: The platform cross-references the HTTP Accept-Language header array, the active keyboard input layout (queried via the Keyboard API), and UI navigation velocities against typical localized behavioral patterns to detect anomalous access attempts.

Section 5: Strategic Synthesis

The digital governance of online extremism operates through an interconnected framework of public criminal statutes, corporate acceptable use policies, and network security protocols. Rather than functioning in isolation, these three layers create an integrated enforcement system that addresses the jurisdictional limits of sovereign legal systems.

Public criminal statutes (such as 18 U.S.C. § 2331 and 28 C.F.R. § 0.85) define the sovereign baseline of state enforcement. The state's reach within domestic borders is constrained by the First Amendment and the *Brandenburg* incitement standard, precluding the federal government from creating domestic terrorist designation lists or proscribing non-imminent radical political speech.

However, the First Amendment rights confirmed in *Moody v. NetChoice* empower private platforms to exercise editorial discretion. Platforms establish lower harm thresholds, bridge the domestic/international statutory divide, and proactively suppress extremist manifestos, iconography, and radicalization networks that the state cannot prosecute directly.

This privatized speech-governance framework is further shaped by international regulatory divergence. The European Union’s Digital Services Act (Articles 34 and 35) and the Terrorist Content Online Regulation penalize systemic negligence and compel the rapid mitigation of online extremism. This creates an operational conflict with U.S. state common-carrier initiatives.

To navigate these competing cross-border mandates, platforms deploy advanced network security architectures. Where legal boundaries blur across globalized digital infrastructure, technical enforcement protocols—ranging from Anycast RTT latency triangulation and TLS JA4 fingerprinting to WebRTC candidate enumeration and ambient RF triangulation—function as digital border controls. These systems translate complex, multi-jurisdictional legal frameworks into code, algorithmically partitioning the global internet to enforce distinct legal and moderation

standards at the physical network edge.

Works cited

1. 2, https://s3.amazonaws.com/storage.citizensforethics.org/wp-content/uploads/2019/09/09175804/Pages-from-Pages-from-Release-last-pages1.pdf 2. United States of America, Plaintiff-appellee, v. Randy Graham, https://law.justia.com/cases/federal/appellate-courts/F3/275/490/592371/ 3. Designating domestic terrorist individuals or groups - Calhoun, https://calhoun.nps.edu/server/api/core/bitstreams/e0d24520-bec5-4e36-93e3-c0cca0b0c0d6/content 4. forum - motifator.com, https://www.motifator.com/index.php/forum/mem/viewreply/509477/ 5. 28 CFR Part 50 -- Statements of Policy - eCFR, https://www.ecfr.gov/current/title-28/chapter-I/part-50 6. Moody Decision Confirms First Amendment Protects Online Platforms, https://www.dwt.com/insights/2024/07/scotus-moody-ruling-a-win-for-online-platforms 7. Possibilities for Social Media Regulation After Moody v. NetChoice, https://proceedings.nyumootcourt.org/2024/12/editorial-discretion-and-doxing-possibilities-for-social-media-regulation-after-moody-v-netchoice-llc/ 8. 22-277 Moody v. NetChoice, LLC (07/01/2024) - Supreme Court, https://www.supremecourt.gov/opinions/23pdf/22-277_d18f.pdf 9. Using the DSA to Study Platforms - Verfassungsblog, https://verfassungsblog.de/dsa-platforms-digital-services-act/ 10. Article 34, the Digital Services Act (DSA), https://www.eu-digital-services-act.com/Digital_Services_Act_Article_34.html