FROM HIERARCHIES TO ALGORITHMS: FILLING THE FEDERAL DOMESTIC TERRORISM GAP

Camille A. Cox*

I. INTRODUCTION

In recent years, federal investigations and public reports have connected acts of mass violence not to organized extremist groups, but to individuals radicalized through social media platforms and algorithmically amplified content.[1] These emerging pathways challenge long-standing assumptions about how extremist actors organize and expose a gap in the current federal counterterrorism legal framework.

In the aftermath of September 11, Congress structured federal counterterrorism law around threats associated with foreign organizations and coordinated networks.[2] While lawmakers later defined "domestic terrorism" to describe certain acts of ideologically motivated violence occurring within the United States, they declined to enact a corresponding federal criminal offense.[3] As a result, prosecutors confronting domestic extremism must rely on a patchwork of hate-crime, firearms, conspiracy, and obstruction statutes.[4]

---

* Juris Doctor Candidate at Southern University Law Center, May 2027. I would like to thank my faculty advisor, Professor Jason Thrower, for his guidance and support. I am also deeply thankful to my mentors, professors, and loved ones for their continued encouragement throughout this process.

1. *See* S. Comm. on Homeland Sec. & Governmental Affairs, 117th Cong., Domestic Terrorism and Social Media: The Federal Government's Response to the Rise of Violent Extremism 8 (Majority Staff Rep. 2022), https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/221116_HSGACMajorityReport_DomesticTerrorism&SocialMedia.pdf (last visited Mar. 2, 2026).

2. *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272; 18 U.S.C. §§ 2339A–2339B.

3. *See* MARY MCCORD, *FILLING THE GAP IN OUR TERRORISM STATUTES* 2–3 (Program on Extremism, George Washington Univ., 2019), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/McCord%20Filling%20the%20Gap.pdf.

4. *See* MCCORD, *supra* note 3, at 2–3; *see also* S. Comm. on Homeland Sec. & Governmental Affairs, *supra* note 1, at 17.

At the same time, the model of terrorism assumed by federal law has become increasingly outdated. Traditional counterterrorism statutes were built around identifiable leaders, formal hierarchies, and coordinated planning.[5] Today, many extremist actors are radicalized through loosely connected online networks rather than through membership in established organizations.[6] Social-media platforms and recommendation systems are designed to maximize engagement rather than evaluate risk, yet they increasingly function as the primary pathways through which violent ideologies spread.[7] Federal law, however, continues to assume cooperation among human actors and organizational intent, even as emerging threats arise from digital environments where no formal group exists to hold responsible.[8]

This Article argues that closing the domestic terrorism gap requires three complementary reforms: a narrowly tailored federal domestic terrorism statute, a statutory clarification distinguishing algorithmic amplification from passive hosting under Section 230, and enhanced interagency coordination mechanisms. Part II traces how the statutory gap emerged. Part III examines how digital networks have transformed domestic extremism and illustrates the consequences through the January 6 attack and the Buffalo supermarket shooting. Part IV proposes a domestic terrorism statute and examines its constitutional boundaries. Part V addresses platform immunity and algorithmic accountability under Section 230. Part VI proposes interagency coordination mechanisms to integrate the federal response.

5. *See* MCCORD, *supra* note 3, at 2–3.

6. *See U.S. Dep't of Homeland Sec., Office of Intelligence & Analysis, Homeland Threat Assessment 2025, at 2–3 (2024), https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf (last visited Feb. 25, 2026).*

7. *See* S. Comm. on Homeland Sec. & Governmental Affairs, *supra* note 1, at 6.

8. *See* MCCORD, *supra* note 3, at 2–3.

II. BACKGROUND

A. Statutory Framework

Federal law recognizes and defines "domestic terrorism," but does not provide a corresponding criminal offense. Congress formally defined domestic terrorism in the USA PATRIOT Act of 2001, which amended the federal criminal code to include the following definition: "[T]he term 'domestic terrorism' means activities that—(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended—(i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States."[9] Codified at 18 U.S.C. § 2331(5), this provision provides a broad definitional framework but does not create a substantive offense. Instead, it functions as a reference point for federal agencies such as the FBI and the Department of Homeland Security to track and categorize threats, rather than a charge prosecutors may bring in court.[10]

The absence of a domestic terrorism charge stands in distinct contrast to the statutory framework for international terrorism. Under 18 U.S.C. §§ 2339A–2339B, Congress created the material support statutes, which criminalize providing money, training, personnel, or other resources to designated foreign terrorist organizations, even in the absence of direct participation in violent acts.[11] Courts have consistently upheld the range of these statutes against constitutional challenges, most notably in *Holder v. Humanitarian Law Project*, where the Supreme Court rejected First Amendment objections to the ban on providing training and expert advice.[12] Together, these statutes reflect

9. USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 802, 115 Stat. 272, 376 (codified at 18 U.S.C. § 2331(5)).

10. *See Fed. Bureau of Investigation & U.S. Dep't of Homeland Sec., Domestic Terrorism: Definitions, Terminology, and Methodology 1 (2020); McCord, supra* note 3, at 2–3.

11. *18 U.S.C. §§ 2339A–2339B (2018).*

12. *Holder v. Humanitarian Law Project*, 561 U.S. 1, 28–36 (2010).

Congress's intent to give prosecutors a range of authority when addressing terrorism with a foreign relationship, in contrast to the limited options available in domestic terrorism cases.

This gap in substantive law has produced inconsistencies and disparities in enforcement, as prosecutors have wide discretion to decide whether conduct will be labeled as terrorism or prosecuted as ordinary crimes.[13]

III. THE DIGITAL AGE AND THE EVOLUTION OF DOMESTIC EXTREMISM

The domestic terrorism threat environment in the United States remains high, characterized increasingly by lone offenders radicalized online rather than through membership in organized groups or formal hierarchies.[14] Federal law enforcement now tracks domestic extremism across several ideological threat categories — from racially motivated violence to anti-government extremism — reflecting a landscape far more decentralized than the organized movements of prior decades.[15] Social media platforms, online forums, and algorithm-driven recommendation systems now provide pathways for radicalization that are faster, broader, and more difficult to detect than traditional recruitment methods.[16] This Part examines that transformation by tracing the move from organized extremism to online radicalization, defining the process of algorithmic radicalization, and analyzing its real-world consequences through recent U.S. case studies.

A. Algorithmic Radicalization and the Digital Pathway to Extremism

Digital technologies have fundamentally altered how individuals encounter, consume, and internalize extremist ideas.[17] Unlike earlier forms of online radicalization that required deliberate participation in chatrooms or message boards,

13. *See* MCCORD, *supra* note 3, at 1–2.

14. *See* U.S. Dep't of Homeland Sec., *supra* note 6, at 2–3.

15. *See* Fed. Bureau of Investigation & U.S. Dep't of Homeland Sec., *supra* note 10, at 2–3.

16. *See* S. Comm. on Homeland Sec. & Governmental Affairs, *supra* note 1, *at 6,* 82.

17. *Id. at 82.*

algorithmic radicalization occurs when automated recommendation systems expose users to increasingly extreme content without any intentional search.[18] Social media platforms like YouTube, TikTok, and Facebook rely on engagement-based algorithms that prioritize content most likely to capture attention, often material that is polarizing, sensational, or emotionally charged.[19] Over time, these systems can generate a personalized stream of violent and extremist content that gradually reshapes a user's worldview and increases the risk of radical beliefs and violent intent.[20]

Algorithms are designed to maximize engagement and advertising revenue rather than evaluate the social impact of the content they promote, leading platforms originally built for entertainment and social connection to function as primary pathways for the spread of extremist content.[21]

B. The Offline Impact of Online Extremism

The January 6th attack at the U.S. Capitol and the May 2022 Buffalo supermarket shooting illustrate how this statutory gap produces concrete failures of accountability.[22] Federal investigators found that extremist groups including the Oath Keepers and Proud Boys coordinated via social media to organize and execute the attack on the Capitol.[23] Despite conduct that clearly satisfied the definitional elements of 18 U.S.C. § 2331(5), no participant was charged with domestic terrorism. Federal prosecutors instead relied on obstruction, conspiracy, and assault statutes — tools capable of addressing discrete criminal acts but

18. *See* S. Comm. on Homeland Sec. & Governmental Affairs, *supra* note 1, at 99–100*; see also* REBECCA LEWIS, ALTERNATIVE INFLUENCE: BROADCASTING THE REACTIONARY RIGHT ON YOUTUBE *35–36 (Data & Soc'y Research Inst. 2018), https://datasociety.net/wp-content/uploads/2018/09/DS_Alternative_Influence.pdf (*last visited Mar. 23, 2025*).*

19. *See* S. Comm. on Homeland Sec. & Governmental Affairs, *supra note* 1, at 99–100.

20. *Id*.

21. *Id.*

22. *See* S. Comm. on Homeland Sec. & Governmental Affairs, *supra* note 1, at 17-20.

23. *Id.* at 19.

ill-suited to capturing the ideological nature of the violence.[24] As Mary McCord has observed, this gap creates a concrete enforcement asymmetry: conduct that would constitute terrorism under federal law if connected to a foreign organization is prosecuted as ordinary crime when it originates domestically.[25]

The Buffalo supermarket shooting presents a parallel failure. The New York Attorney General concluded that the Buffalo shooter was first indoctrinated and radicalized through online platforms, where fringe websites and unmoderated forums exposed him to racist and violent content that deepened his extremist ideology and enabled him to plan and publicize his attack.[26] As in the January 6 prosecutions, federal authorities were limited to hate-crime and firearms charges despite the shooter's explicit ideological motivation and the terroristic impact of the act.[27] Together these cases reveal not a prosecutorial failure but a legislative one — and one that the digital transformation of radicalization has made impossible to ignore.

IV. BRIDGING THE LEGAL GAP: ADAPTING DOMESTIC TERRORISM TO THE DIGITAL AGE

While courts remain constrained by constitutional limits on expanding criminal liability, Congress retains the authority and responsibility to modernize terrorism statutes to reflect how domestic extremism now develops. Existing counterterrorism statutes — including the material support provisions of 18 U.S.C. §§ 2339A–2339B — require either coordinated conduct or a nexus to a designated foreign terrorist organization, leaving no federal charging vehicle for ideologically motivated violence committed by individuals who radicalize outside any formal organizational

24. *See* 18 U.S.C. § 2331(5); *see also* McCord, *supra* note 3, at 1–2; Sacco, *supra* note 22, at 1.

25. McCord, *supra* note 3, at 1–2.

26. N.Y. Att'y Gen., *Investigation into the Role of Online Platforms in the May 14, 2022 Buffalo Shooting* 1–4, 23–26 (2022), https://ag.ny.gov/sites/default/files/buffaloshooting-onlineplatformsreport.pdf (last visited Mar. 8, 2026).

27. *See* S. Comm. on Homeland Sec. & Governmental Affairs, *supra* note 1, at 19–20; *see also* McCord, *supra* note 3, at 1–2.

structure.[28] Filling that gap must navigate the tension between effective counterterrorism enforcement and First Amendment protections. This Part examines those constitutional boundaries and proposes a framework for statutory reform that respects both imperatives.

A. Constitutional Boundaries

The Supreme Court's decision in *Brandenburg v. Ohio* established that government may not punish advocacy of the use of force or violation of law unless such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.[29] Any domestic terrorism statute must respect this boundary by requiring proof of specific intent to commit violence and a substantial step toward imminent harm — not mere consumption of extremist content or abstract ideological agreement.[30]

Applied to the digital context, this framework means that consuming extremist content, participating in online forums, or even expressing support for violent ideologies remains protected absent concrete steps toward violence. A properly constructed domestic terrorism statute should treat digital activity as evidence of motive, planning, and intent when paired with actions such as acquiring weapons, surveilling targets, drafting operational plans, or attempting to recruit accomplices, not as an independent basis for liability.[31] Courts routinely admit internet search histories, social media posts, and online communications to establish intent in criminal prosecutions for terrorism, murder, and other violent

28. 18 U.S.C. §§ 2339A–2339B (2018); *see also* McCord, *supra* note 3, at 2–3.

29. Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).

30. *See Scales v. United States*, 367 U.S. 203, 229–30 (1961) (holding that membership in an organization advocating violent overthrow may be punished only where the defendant specifically intends to accomplish the organization's aims by resort to violence); *Noto v. United States*, 367 U.S. 290, 298–300 (1961).

31. *United States v. Abu-Jihaad*, 630 F.3d 102, 133 (2d Cir. 2010) (holding that evidence of pro-jihadist materials was admissible to establish defendant's motive and intent in communicating classified information that could facilitate harm to his own vessel).

crimes.[32] Algorithmic radicalization evidence would serve the same evidentiary function: demonstrating the formation and progression of criminal intent, instead of substituting for it.

Three additional constitutional protections are essential. First, the statute must require that the defendant act with at least reckless disregard for the likelihood that their conduct would result in violence — satisfying the constitutional minimum established in *Counterman* — and should ideally demand specific intent to commit violence rather than mere negligence or objective reasonable-person liability.[33] Second, it must incorporate an imminence requirement, limiting liability to cases where the defendant has progressed beyond abstract planning to concrete preparation for imminent harm.[34] Third, it must require proof of a substantial step — such as acquiring weapons, conducting surveillance, or drafting target lists — that corroborates the defendant's intent and distinguishes genuine threats from empty words.[35]

B. Statutory Design

Building on these constitutional foundations, Congress should enact a narrowly tailored domestic terrorism offense: A person commits domestic terrorism if they knowingly engage in conduct that: (1) involves an act dangerous to human life that violates federal or state criminal law; and (2) is committed with the specific intent to: (a) intimidate or coerce a civilian population; (b) influence the policy of a government by intimidation or

32. *See Mehanna*, 735 F.3d at 41; *see also Abu-Jihaad*, 630 F.3d 102.

33. *See Elonis v. United States*, 575 U.S. 723, 738–40 (2015); *see also Counterman v. Colorado, 600 U.S. 66, 69 (2023).*

34. *See Hess v. Indiana*, 414 U.S. 105, 108–09 (1973) (holding that advocacy of illegal action at some indefinite future time is constitutionally protected, and that the First Amendment bars punishment absent evidence that speech was intended and likely to produce imminent disorder).

35. *See generally United States v. Mehanna*, 735 F.3d 32, 41 (1st Cir. 2013) (affirming conviction where defendant's concrete preparatory conduct corroborated intent to provide material support to terrorism); *United States v. Gladish*, 536 F.3d 646, 650 (7th Cir. 2008).

coercion; or (c) affect the conduct of a government by mass destruction, assassination, or kidnapping.[36]

This framework adopts the definitional structure already codified at 18 U.S.C. § 2331(5) but converts it into a substantive criminal offense.[37] It requires both a predicate criminal act and proof of terrorism-specific intent, ensuring that ordinary violent crimes are not swept into terrorism liability merely because they produce fear or attract public attention, and guarding against the risk that enforcement could be used to target disadvantaged groups or political protestors.[38] The objection that existing law already punishes all relevant conduct, and that no terrorist has escaped accountability for want of a charging statute, misses the point.[39] Punishment without terrorism accountability is not an adequate substitute. It obscures the ideological nature of the harm, produces inconsistent enforcement, and denies the law its expressive function in treating violence designed to coerce civilian populations or influence government action as categorically distinct from ordinary crime.[40]

Applied to January 6 and Buffalo, this statute would have enabled prosecutors to charge conduct that plainly satisfied its

36. The proposed offense adapts the definitional elements of 18 U.S.C. § 2331(5) and is modeled in part on the framework proposed in McCord, *supra* note 3, at 3–4. *See also* 18 U.S.C. § 2332b (providing a charging framework for acts of terrorism transcending national boundaries that served as a model for McCord's proposal).

37. 18 U.S.C. § 2331(5) (2018).

38. *See* McCord, *supra* note 3, at 3–5 (proposing a narrowly tailored statute requiring terrorism-specific intent to distinguish ideologically motivated violence from ordinary violent crime); Sacco, *supra* note 22, at 17–19.

39. Brian Michael Jenkins, *Five Reasons to Be Wary of a New Domestic Terrorism Law*, RAND (Feb. 24, 2021), https://www.rand.org/pubs/commentary/2021/02/five-reasons-to-be-wary-of-a-new-domestic-terrorism.html (last visited Mar. 9, 2026), *quoted in* Sacco, *supra* note 22, at 18; *see also* Sacco, *supra* note 22, at 18 (noting the related argument that existing statutes are sufficient because domestic terrorists have been successfully prosecuted under other federal laws).

40. *See* McCord, *supra* note 3, at 1 (arguing that the statutory gap fails to identify the distinct harm of ideologically motivated violence and produces inconsistent treatment of comparable conduct); Sacco, *supra* note 22, at 17 (noting the argument that a domestic terrorism charge would allow prosecutors to characterize conduct as an issue of national security rather than ordinary crime, reflecting the terroristic nature of the harm).

elements — ideologically motivated violence directed at coercing civilian populations or influencing government action — rather than relying on surrogate offenses that obscured the terroristic nature of each attack.[41] That distinction is not merely a matter of labels. A terrorism charge carries different sentencing exposure, triggers distinct investigative authorities, and — critically — conveys to the public, to future offenders, and to the historical record that the conduct was not ordinary crime but an attack on democratic society itself.[42] When the law fails to call terrorism by its name, it forfeits both its deterrent function and its expressive capacity to identify the distinct harm at issue.[43]

V. PLATFORM IMMUNITY AND ALGORITHMIC ACCOUNTABILITY

Section 230 of the Communications Decency Act shields platforms from most liability arising from user content, even when algorithmic systems actively shape how that content spreads. Understanding Section 230's scope and its limits is essential to closing the domestic terrorism gap.

A. Section 230's Immunity Problem

Section 230(c)(1) provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information

41. *See* McCord, *supra* note 3, at 1 (noting that perpetrators of ideologically motivated mass violence are charged with "weak" surrogate offenses that fail to reflect the terroristic nature of the conduct); Sacco, *supra* note 22, at 6–7 (documenting that despite FBI characterization of January 6 as domestic terrorism, most federal charges against participants ranged from vandalism to seditious conspiracy and did not include domestic terrorism or a terrorism sentencing enhancement); N.Y. Att'y Gen., *Investigation into the Role of Online Platforms in the May 14, 2022 Buffalo Shooting* (2022), https://ag.ny.gov/sites/default/files/buffaloshooting-onlineplatformsreport.pdf (last visited Mar. 8, 2026) (finding that federal authorities were limited to hate-crime and firearms charges despite the shooter's explicit ideological motivation).

42. Sacco, *supra* note 22, at 6–7, 17.

43. DAN M. KAHAN, *What Do Alternative Sanctions Mean?*, 63 U. CHI. L. REV. 591, 593 (1996) (arguing that punishment is not merely a mechanism for inflicting suffering but a social convention that expresses moral condemnation, and that the form of sanction communicates to the community the seriousness of the wrong)

content provider."[44] This provision prevents platforms from liability under theories treating them as publishers of third-party content.[45]

But today's platforms operate nothing like the passive hosts Congress envisioned in 1996. Modern platforms do not simply host content — they actively curate what users see through sophisticated recommendation algorithms.[46] When YouTube's algorithm suggests increasingly extreme videos or Facebook's system prioritizes inflammatory posts, platforms make editorial choices about what to amplify and to whom.[47] Section 230, however, continues to treat these active curation decisions as equivalent to neutral hosting, even when algorithmic systems systematically expose vulnerable users to radicalizing content.[48]

B. Distinguishing Amplification from Hosting

Platforms should retain immunity for content they merely store. This immunity enables platforms to host user speech without becoming insurers against all harms. When a platform's automated system selects specific content to promote to specific users based on predicted engagement, the platform makes an affirmative editorial choice that reflects its own judgment, implemented through code rather than human editors.[49] Where that choice foreseeably facilitates harm — by systematically

44. 47 U.S.C. § 230(c)(1)

45. *Id*.

46. 47 U.S.C. § 230 (1996); *see* S. Comm. on Homeland Sec. & Governmental Affairs, *supra* note 1 (documenting that major platforms employ recommendation algorithms that actively shape user exposure to content in ways Congress did not contemplate in 1996).

47. *See* S. Comm. on Homeland Sec. & Governmental Affairs, *supra* note 1, at 98–116 (documenting that Meta and YouTube employ engagement-based recommendation algorithms that prioritize inflammatory and extreme content).

48. *See* DANIELLE KEATS CITRON & BENJAMIN WITTES, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 417–22 (2017); *see also Gonzalez v. Google LLC, 598 U.S. 617, 622 (2023) (declining to address whether § 230 immunity applies to algorithmic recommendations and resolving the case on narrower Anti-Terrorism Act grounds).*

49. *See* CITRON & FRANKS, *supra* note 54; *see also Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1090–92 (9th Cir. 2021).

exposing users to radicalizing content — traditional tort principles would permit liability.[50]

Courts have recently begun recognizing this distinction. In *Lemmon v. Snap, Inc.*, the Ninth Circuit held that Snapchat's "Speed Filter" which overlaid speed on photos and allegedly encouraged dangerous driving did not qualify for Section 230 protection because it constituted the platform's own product design rather than third-party content.[51] The Supreme Court declined to resolve this question in *Gonzalez v. Google LLC*, leaving significant doctrinal ambiguity.[52] That ambiguity has real consequences: treating algorithmic promotion as indistinguishable from traditional publishing allows platforms to profit from engagement with extremist content while avoiding accountability for the foreseeable effects of their design choices.[53]

Congress could clarify that algorithmic recommendation constitutes a distinct category of conduct — separate from passive hosting — that may give rise to limited liability when it materially contributes to foreseeable harm.[54] Congressional Research Service analysis has confirmed that existing Section 230 doctrine leaves unresolved whether algorithmic recommendations constitute publisher activity subject to immunity or a distinct form of platform conduct outside Section 230's protections.[55] Liability would arise only where the platform's algorithmic system actively

50. *See* RESTATEMENT (SECOND) OF TORTS § 302 (1965); *see also* CITRON & WITTES, *supra* note 54, at 417–22 (arguing that § 230 immunity should not extend to platforms that knowingly enable illegal activity or whose business model facilitates harm, and proposing a reasonable steps standard to cabin the immunity).

51. *Lemmon*, 995 F.3d at 1090–92.

52. See Gonzalez v. Google LLC, 598 U.S. 617, 622 (2023) (declining to address Section 230's application to algorithmic recommendations and resolving case on narrower Anti-Terrorism Act grounds).

53. *See JACK M. BALKIN, How to Regulate (and Not Regulate) Social Media, 1 J. FREE SPEECH L. 71 (2021).*

54. *See* DANIELLE KEATS CITRON & MARY ANNE FRANKS, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform*, 2020 U. CHI. LEGAL F. 45 (proposing narrow exceptions to Section 230 immunity for platforms whose design choices foreseeably facilitate harm).

55. *See* Eric N. Holmes, Cong. Rsch. Serv., R47753, *Liability for Algorithmic Recommendations* (Oct. 12, 2023), https://www.congress.gov/crs-product/R47753 (last visited Mar. 15, 2026).

amplified content that foreseeably facilitated violence, the platform knew or should have known of this risk, and the amplification was a proximate cause of the harm.[56] This standard imposes no greater burden than ordinary negligence principles applied in any other commercial context.

C. Coordination with Criminal Law Reform

A domestic terrorism statute and Section 230 clarification are mutually reinforcing. The statute defines the conduct that platforms might foreseeably facilitate; Section 230 clarification establishes that facilitating such conduct through algorithmic amplification does not qualify for absolute immunity. Congress should also require major platforms to disclose to independent regulators the general logic governing their recommendation systems, publish regular transparency reports measuring user exposure to extremist content, and provide qualified researchers with secure access to anonymized data to study online radicalization patterns.[57] The European Union's Digital Services Act demonstrates that such requirements can be framed as regulatory accountability measures rather than content control.[58] Without such visibility, lawmakers and law enforcement agencies cannot assess when algorithmic amplification meaningfully facilitates extremist mobilization.[59] Such transparency obligations are constitutionally defensible — they regulate platform conduct rather than speech and impose only factual disclosure requirements of the kind courts have consistently upheld.[60]

---

56. *See* FRANCESCA KENNEDY, *Harmful Connections: How Tort Law Can Address Algorithmic Account Recommendation Harms and Protect Youth Social Media Users*, 33 AM. U. J. GENDER SOC. POL'Y & L. 98, 106, 121–22 (2025); *see also* RESTATEMENT (SECOND) OF TORTS § 302 (1965); *cf.* RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM § 29 (AM. L. INST. 2010).

57. *See* S. Comm. on Homeland Sec. & Governmental Affairs, *supra* note 1, at 98–116 (recommending platform transparency and researcher data access requirements).

58. Council Regulation 2022/2065, *Digital Services Act*, 2022 O.J. (L 277) 1 (EU).

59. *See* Sacco, *supra* note 22, at 21–22.

60. *See* Zauderer v. Off. of Disciplinary Couns., 471 U.S. 626, 651 (1985) (holding that compelled disclosure of factual information does not violate the

VI. INTERAGENCY COORDINATION

Effective responses to digitally mediated extremism require more than statutory reform or platform regulation; they require a federal enforcement strategy capable of operating across institutional and jurisdictional boundaries. Responsibility for addressing domestic extremism is currently divided among multiple federal agencies with distinct mandates and operational roles. The Department of Homeland Security (DHS) focuses primarily on threat assessment and prevention, the Federal Bureau of Investigation (FBI) leads criminal investigations, and the Department of Justice (DOJ) controls charging decisions and prosecutorial strategy.[61] Although these missions frequently overlap in practice, they are often pursued through separate processes and information systems, limiting the government's ability to respond cohesively to emerging threats.

This institutional divide has tangible consequences. The Government Accountability Office (GAO) has repeatedly warned that the absence of a unified federal strategy undermines the government's ability to identify domestic extremist threats early and respond in a timely manner.[62] Information relevant to radicalization trajectories is frequently compartmentalized: DHS may track online trends and emerging extremist narratives, the FBI may possess case-specific investigative intelligence, and DOJ evaluates prosecutorial viability under statutes that were not designed to account for digital facilitation.[63] Without formal

First Amendment where reasonably related to a substantial governmental interest); Milavetz, Gallop & Milavetz, P.A. v. United States, 559 U.S. 229, 249–53 (2010) (applying Zauderer to uphold disclosure requirements as constitutionally valid were directed at preventing consumer deception through accurate factual statements).

61. U.S. Dep't of Homeland Sec., Office of Intelligence & Analysis, *Homeland Threat Assessment 2025*, at 2–5 (2024), https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf (last visited Feb. 25, 2026); Fed. Bureau of Investigation & U.S. Dep't of Homeland Sec., *Domestic Terrorism: Definitions, Terminology, and Methodology* (2020), https://www.fbi.gov/file-repository/domestic-terrorism-definitions-terminology-methodology.pdf (last visited Mar. 2, 2026).

62. GAO-23-104720, *supra* note 28, at 52–53.

63. *See* GAO-23-104720, *supra* note 28, at 52–53; McCord, *supra* note 3, at 5–6.

mechanisms to integrate these perspectives, early warning signs may never translate into actionable intervention.

These coordination failures are especially pronounced in the digital context. Algorithmic radicalization rarely occurs in a single forum or within a discrete investigative window. Instead, it develops gradually across multiple platforms and over extended periods of time, generating fragmented data that does not align neatly with any one agency's traditional concern.[64] The result is a structural mismatch: the very agencies best positioned to detect early radicalization signals operate under mandates and information systems that were never designed to communicate with one another about threats that develop gradually, anonymously, and across jurisdictional lines.[65]

The January 6 attack and the Buffalo shooting illustrate this failure concretely. In both cases, relevant warning signs were visible across agency lines before violence occurred. DHS had documented the growth of online extremist networks and the radicalization pathways associated with the ideologies driving each attack.[66] The FBI possessed investigative intelligence regarding specific actors and platforms. Yet charging decisions at DOJ were made under statutes that had no mechanism for incorporating that upstream threat assessment data — because no formal structure required or enabled it.[67] The result in both cases was prosecution of the violent act in isolation, stripped of the

64. U.S. Dep't of Homeland Sec., Office of Intelligence & Analysis, *Homeland Threat Assessment 2025*, at 2-3 (2024), https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf (last visited Feb. 25, 2026); N.Y. Att'y Gen., *Investigation into the Role of Online Platforms in the May 14, 2022 Buffalo Shooting* (2022), https://ag.ny.gov/sites/default/files/buffaloshooting-onlineplatformsreport.pdf (last visited Mar. 8, 2026).

65. *See GAO-23-104720, supra note 28, at 52–53 (finding that FBI and DHS track different domestic terrorism information specific to their respective missions and have not assessed whether existing agreements fully reflect their charge to jointly prevent domestic terrorism attacks).*

66. *See* S. Comm. on Homeland Sec. & Governmental Affairs, *supra* note 1, at 38–43; U.S. Dep't of Homeland Sec., Office of Intelligence & Analysis, *Homeland Threat Assessment 2025*, *supra* note 73, at 2–3.

67. *See* GAO-23-104720, *supra* note 28; McCord, *supra* note 3, at 5–6.

ideological and facilitative context that gave it its terroristic character.[68]

As a result, no single agency is structurally positioned to assemble a complete picture of risk before violence occurs. Intelligence about emerging narratives may remain disconnected from investigative leads, while prosecutorial decision-making occurs downstream after harm has already materialized.[69] Scholars and former national security officials have cautioned that this reactive posture leaves federal counterterrorism efforts perpetually one step behind digitally mediated threats, intervening only after violence has occurred rather than disrupting pathways to mobilization.[70]

Congress should establish a standing interagency task force with authority to develop standardized protocols for assessing algorithmic radicalization threats, share intelligence regarding emerging extremist narratives across platforms, and coordinate investigative and prosecutorial responses to domestic terrorism cases.[71] Such mechanisms would integrate DHS threat assessments with FBI investigative leads and DOJ charging decisions, enabling federal authorities to assemble a complete picture of risk before violence occurs. Without durable coordination structures that account for the decentralized and algorithmically driven nature of contemporary radicalization, federal counterterrorism policy will remain reactive rather than preventive.[72]

68. *See* McCord, *supra* note 3, at 1; Sacco, *supra* note 22, at 6–7.

69. *See* GAO-23-104720, *supra* note 28; Sacco, *supra* note 22, at 21–22.

70. *See McCord, supra* note 3, at 5–6*; Sacco, supra* note 22, at 21–22.

71. *See* Michael E. DeVine, John W. Rollins & Lisa N. Sacco, Cong. Rsch. Serv., R47229, *Intelligence Coordination on Domestic Terrorism and Violent Extremism: Background and Issues for Congress* 14 (Sept. 1, 2022), https://www.congress.gov/crs-product/R47229 (last visited Mar. 15, 2026) (documenting congressional proposals to establish interagency task forces with authority to coordinate investigative and prosecutorial responses to domestic terrorism threats); *see also* GAO-23-104720, *supra* note 28, at 53.

72. *See* GAO-23-104720, *supra* note 28, at 53.

VI. CONCLUSION

On January 6, 2021, thousands of individuals who had never attended a recruitment meeting, never joined a formal organization, and never received direction from an identifiable leader stormed the United States Capitol. Eighteen months later, a young man who had spent months consuming algorithmically amplified racially extremist content on platforms he never deliberately sought walked into a Buffalo supermarket and opened fire. In both cases, federal prosecutors charged what they could — obstruction, conspiracy, hate crimes, firearms offenses — because federal law gave them nothing else. The conduct satisfied the statutory definition of domestic terrorism. The charge did not exist.

That is not a prosecutorial failure. It is a legislative one. Congress defined domestic terrorism in 2001 and then declined to make it a crime, leaving the definition to function as a label rather than a legal tool. In the two decades since, the mechanisms of radicalization have shifted from human recruiters and organizational hierarchies to engagement-driven algorithms that systematically expose users to escalating extremist content without their awareness or consent. Federal law has not moved with them.

The reforms proposed in this Article do not require dismantling the First Amendment or abandoning the architecture of internet law. A domestic terrorism statute grounded in specific intent, imminence, and a substantial step toward violence punishes conduct, not belief. A statutory clarification distinguishing algorithmic amplification from passive hosting holds platforms accountable for their own design choices, not for the expressive content generated by their users. Interagency coordination mechanisms ensure that threat assessment, investigation, and prosecution operate as a unified response rather than sequential and disconnected functions. Algorithmic transparency obligations give that entire system the visibility it currently lacks.

The law has confronted technological disruption before and adapted. After September 11, Congress reshaped the entire architecture of federal counterterrorism law within months. The threat today is different — more diffuse, more digitally mediated,

and in some ways harder to see — but it is no less real. Every year that federal law remains calibrated to the terrorism of 2001 is another year in which the mechanisms that produced January 6 and Buffalo operate without meaningful legal constraint. The cost of that delay will not be theoretical. It will be measured in the next attack that federal law sees clearly only in hindsight.