

# Confronting the Disinformation Engine

Insights by Professor Barbara McQuade

## Overview

Digital platforms have transformed the way information circulates, making the rapid spread of misinformation and disinformation a central legal concern. Disinformation—deliberately false or manipulated information—and misinformation—incorrect or misleading information shared without harmful intent—present complex challenges for national security and the rule of law. In her discussion, Professor Barbara McQuade, a former U.S. attorney and national security prosecutor and now a professor of National Security Law at the University of Michigan Law School, explains why these phenomena have become pressing legal issues.

---

## I. Defining the Landscape

- Disinformation vs. Misinformation
    - *Disinformation* is intentionally crafted falsehood intended to deceive, while *misinformation* is inaccurate or misleading information that is sometimes shared without harmful intent.
  - The Digital Environment:
    - Digital platforms facilitate the near-instantaneous distribution of content to vast audiences, heightening the risk of widespread false narratives.
  - National Security Implications:
    - Professor McQuade emphasizes that disinformation poses one of the most significant threats to national security, drawing on her extensive experience in national security prosecutions.
-

## II. Algorithmic Amplification as a Battleground

- Role of Social Media Algorithms:
    - Social media platforms use algorithms designed to maximize user engagement and time on site.
    - This design often inadvertently promotes content that incites anger, outrage, or the spread of conspiracy theories—dynamics that boost traffic and sustain user interaction.
  - Regulatory Opportunities and Concerns:
    - Establishing oversight and technical standards for these algorithms is a promising regulatory strategy. Policymakers might require platforms to adjust algorithmic incentives so that they prioritize accuracy and minimize harmful amplification without compromising user engagement.
  - Case Law and Legal Frameworks:
    - Although specific case law addressing the regulation of software or algorithms controlling speech is still emerging, foundational cases like *Reno v. ACLU*, 521 U.S. 844 (1997) and *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) underscore that any content-related regulation must be narrowly tailored and subject to strict scrutiny.
    - These cases provide guidance on evaluating regulatory measures that affect online speech and indirectly set the stage for the legal debates surrounding algorithmic control.
- 

## III. First Amendment Constraints on Regulation

- Government Regulation and Strict Scrutiny:

- Any government measure that restricts speech—whether directly curbing disinformation or indirectly altering how algorithms operate—must pass the strict scrutiny test. This standard requires:
    - A demonstration of a compelling governmental interest (e.g., protecting national security or public order),
    - A narrow tailoring of the regulation, and
    - Proof that no less restrictive alternative exists.
  - Distinctions for Private Platforms:
    - In contrast, private platforms are not bound by the First Amendment, which is a constraint on government action, granting them broader discretion in content moderation and algorithm design.
  - Balancing Free Speech with Regulation:
    - Professor McQuade notes (quoting Supreme Court Justice Robert Jackson), “The Constitution is not a suicide pact,” which reflects the principle that while the government may impose limits on speech in certain contexts, any restrictions must respect core constitutional rights.
- 

#### IV. Additional Legal Analysis for Practicing Attorneys

##### A. Regulating Software That Controls Speech

- Emerging Jurisprudence:
  - Direct case law specifically addressing the regulation of algorithms or software that controls speech remains limited. However, principles drawn from cases like *Reno v. ACLU* and *Ashcroft v. Free Speech Coalition* provide a benchmark for analyzing any potential regulatory measure affecting online speech.

##### B. Legality of Requiring Disclosure of Bot Accounts

- Legal Considerations:

- Proposals that require disclosure of whether an account is automated (a “bot”) raise important First Amendment questions related to disclosure and the potential chilling effect on speech.
- Requiring disclosure must be justified under a compelling government interest and narrowly tailored to avoid undue burdens on anonymous or pseudonymous expression.
- Relevant Case Law:
  - While there is limited direct case law on bot disclosure, principles from *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), which protects anonymous political speech, suggest that measures mandating disclosure could be vulnerable to First Amendment challenges if they inhibit free expression.

### C. The Right to Pseudonymous or Anonymous Speech

- Constitutional Protections:
    - The U.S. Supreme Court has recognized the importance of anonymous speech—most notably in *McIntyre v. Ohio Elections Commission*—which underscores the value of pseudonymous or anonymous expression in preserving robust public discourse.
  - Balancing Interests:
    - Any regulation that limits anonymous speech must be balanced against the public’s interest in uninhibited debate. Measures that force identification or eliminate the option for pseudonymous participation must be narrowly tailored and serve a compelling interest to withstand constitutional scrutiny.
-

## V. Conclusion

Addressing the challenges of modern digital communication requires an approach that balances technological innovation, regulatory oversight, and constitutional safeguards. Professor Barbara McQuade's discusses the complex interplay between disinformation, algorithmic regulation, and free speech rights. For practicing attorneys, this evolving legal landscape presents both challenges and opportunities—whether advising clients on compliance measures, litigating challenges to regulatory proposals, or shaping future legislative reforms.

Professor Barbara McQuade is a former U.S. attorney and national security prosecutor who now serves as a professor of National Security Law at the University of Michigan Law School.