



May 30, 2025

House Committee on Government Operations and Military Affairs
Vermont State House
115 State Street, Room M106
Montpelier, VT 05633

Re: Senate Bill No. 23 Comments

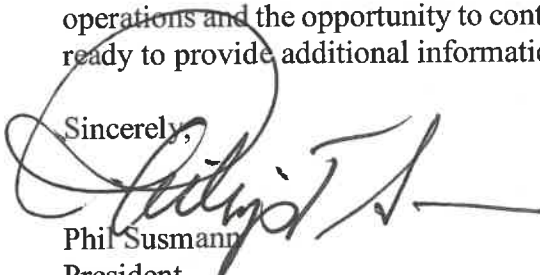
Dear Committee Members:

Thank you for the opportunity to share our research and expertise with the Committee. As a non-profit research organization with extensive experience analyzing and countering malign influence operations, we have worked closely with government, academic, and private-sector partners to understand the tactics, techniques, and impact of such threats. Our team combines operational insight with rigorous research to inform strategies for detection, resilience, and response.

The following comments on Vermont Senate Bill 23 (S.B. 23) reflect key lessons from our work. While we do not offer a specific endorsement, our research and experience demonstrate that proactive efforts to counter malign actors are both effective and essential to preventing, mitigating, and recovering from such activities. We respectfully offer the following observations and believe they may help inform the Committee's consideration of S.B. 23 and other important related legislation.

We appreciate the Committee's attention to the evolving threat posed by malign influence operations and the opportunity to contribute our insights. Our team of subject matter experts stands ready to provide additional information or offer further analysis as needed.

Sincerely,



Phil Susmann
President

Section 1, addition of 17 V.S.A. chapter 35, subchapter 4

§ 2031. Definitions

In **Definition (1) “Deceptive and fraudulent.synthetic media” (p.1, lines 12-15)**, the use of the “reasonable person” standard in the context of media comprehension raises important questions. To our knowledge, Vermont caselaw does not currently provide a definition of what constitutes a “reasonable person” in the context of understanding or interpreting synthetic media. This lack of precedent presents a challenge, as the absence of a clear interpretive standard could complicate enforcement, particularly in cases involving novel or rapidly evolving forms of content.

Malign foreign adversaries frequently operate in the ambiguous space between harmful influence and protected speech, deliberately crafting content that triggers debate over censorship or the suppression of First Amendment rights. Language in the bill such as “injures the reputation of the candidate” or “attempts to unduly influence the outcome of an election” may be vulnerable to these tactics. Such phrases could be used by malign actors in disinformation campaigns to frame enforcement efforts such as criminalizing political speech, satire, or legitimate journalism.

Terms like “injure reputation” and “undue influence” often carry inherently subjective interpretations. Malign actors may exploit this ambiguity by arguing that any campaign communication could be seen as influencing election outcomes—thus further blurring the line between protected political speech and disallowed interference. Extending these arguments to synthetic media as an avenue for protected speech is a foreseeable evolution in their tactics.

Additional Questions for Consideration:

- Could the lack of clarity in what conduct is prohibited open the door to constitutional challenges on the grounds of vagueness under the Due Process Clause?
- Given the common practice among malign actors of obfuscating intent, often through intermediaries, how does the bill address the distinction between actual intent to deceive versus the audience’s perception of deception?
- Would liability hinge on demonstrable intent to mislead, or would merely producing or distributing content that is interpreted as deceptive be sufficient under S.B. 23?

§ 2032. Disclosure of a Deceptive and Fraudulent Synthetic Media

Disclosure requirements (p.2, lines 1-6)

A well-documented tactic used by malign actors is to design content, such as synthetic media, to go viral by encouraging its redistribution through neutral, unsuspecting individuals. Typically, a malign actor creates and initially amplifies the content using networks of bots or paid influencers. The goal is for these neutral actors, which are generally ordinary users with no ill intent, to pick up and share the content within their own networks, thereby increasing its reach and perceived credibility. In these scenarios, the original creator may evade liability altogether, particularly if the content was produced outside the 90-day window defined in the legislation.

The protection afforded to neutral actors who unknowingly share synthetic media introduces should be reviewed, especially given the reliance on the “reasonable person” standard and its lack of definition. The interpretation of what a “reasonable person” should recognize or understand

online is complicated by the nature of digital environments. Social media platforms are designed to promote engagement over discernment, creating conditions that degrade the ability of users to critically assess content before sharing.

Furthermore, malign actors benefit from the fragmented and cross-platform nature of social media. Platforms like BitChute or Rumble might host content that includes a disclosure, but once that content is reposted to mainstream platforms like Facebook or YouTube, often without disclosure, the chain of attribution is broken. This creates a tangled web of potential liability, which malign actors can exploit. In the worst-case scenario, a political candidate might unwittingly share such content, triggering both controversy and confusion around the legality or ethics of their actions.

Malign actors are increasingly turning to machine-generated synthetic media using tools such as DeepSeek and other generative AI systems. The purpose of machine generation is to rapidly outpace detection and response efforts, effectively “flooding the zone” with misleading or ambiguous content. This overwhelms fact-checking and regulatory mechanisms, and contributes to public uncertainty about what is true or false. Undermining trust in the ability to detect or attribute undisclosed content becomes a strategic objective.

(b) Exceptions (pp.2–3, lines 17–21)

Malign actors often view inclusion in mainstream or web-based media outlets as a strategic success, even when their content is labeled or criticized. National media conglomerates and widely read websites have, at times, shared or amplified information that can be traced to foreign influence campaigns. Despite best efforts to apply editorial scrutiny, the amplification itself serves the objectives of malign actors.

Moreover, media platforms frequently accept and distribute paid content or sponsored materials. This creates a commercial pathway for disinformation, including synthetic media that may fall under the definitions outlined in this proposed bill. As synthetic media technologies evolve, the likelihood increases that such materials will be embedded in commercial or journalistic content, intentionally or not, creating further enforcement and attribution challenges.

§ 2033. Penalties

Our research indicates that the economic incentives driving malign influence operations far exceed the potential penalties outlined in this bill. Both nation-state and domestic actors often stand to gain significantly more—financially and strategically—by violating these provisions than they risk losing, even if enforcement is successful.

Moreover, social media platforms profit from the spread of content regardless of its accuracy. Their incentives to comply with regulations or respond to information requests are typically guided less by public interest and more by what they perceive might impact user engagement or advertising revenue. This profit-driven model limits their motivation to curb the dissemination of harmful or deceptive content.

Section 2, addition of 17 V.S.A. chapter 35, subchapter 5

The civil action authorities outlined in **Subchapter 5 (pp. 4–8)** face many of the same enforcement challenges common to the broader field of cybersecurity, particularly when it comes to foreign malign actors. Non-U.S. entities frequently target elections at the state and local levels, not just federal elections, exploiting jurisdictional and legal boundaries to evade accountability. Yet these localized influence operations often serve as building blocks for broader, national-level campaigns.

Machine-generated influence campaigns, which are increasingly favored by malign actors, present additional enforcement difficulties. These automated operations cannot meaningfully respond to legal demands, such as those issued by the Attorney General under this subchapter, further complicating accountability.

Moreover, foreign-owned corporations, including media companies controlled by malign actors, are often central to the spread of disinformation and synthetic media. Their structure and international footprint allow them to bypass or resist the types of enforcement mechanisms proposed in this legislation, reducing the bill’s practical impact on the actors most responsible for harmful influence activities.

Beyond this Bill

Additional Legislative Opportunities

The activities addressed in this bill represent just one aspect of the broader toolkit used by malign actors. Based on our research, effective efforts to counter malign influence typically involve a combination of complementary strategies. Below are five additional areas that frequently intersect with the tactics covered in this legislation:

1. Broader Targeting Beyond Politicians

Election officials, journalists, and private citizens are also targeted by malign actors seeking to influence public perception, incite unrest, or manipulate electoral outcomes. These individuals face similar threats to those directed at political candidates, particularly in the lead-up to elections.

2. Real-Time Detection Technologies

Technologies capable of detecting and labeling synthetic media in real time already exist and continue to evolve. Malign actors exploit rapidly unfolding events such as elections, natural disasters, or crises to overwhelm detection capabilities. Investment in and deployment of real-time monitoring tools can help flag suspicious content before it spreads widely.

3. Platform Responsibility and Social Media’s Central Role

Social media is the primary enabler of synthetic media’s rapid dissemination. Clearly defining and enforcing platform responsibilities can alter the strategic calculus for malign actors. This remains an area of national and international debate, given the central role

that social media companies play in facilitating both legitimate and deceptive communications.

4. Public Education and Awareness

Public awareness campaigns are among the most effective tools for countering synthetic media and other forms of disinformation. Countries such as the Baltic states, Romania, and Moldova have seen success with broad-based public education efforts. For malign actors, an uninformed or accidental share is just as valuable as a malicious one, since engagement algorithms amplify content regardless of intent.

5. Ongoing Legal and Policy Adaptation

Given the rapid evolution of technology and influence tactics, ongoing review and adaptation of legal frameworks and counter-initiatives is essential. Establishing an advisory committee or dedicated office to monitor developments and recommend updates can help ensure policies remain effective and relevant over time.

Other Tools Used by Adverse Actors Beyond Synthetic Media

While synthetic media represents a significant threat, it is only one tool among many used by malign actors to influence public perception and disrupt democratic processes. The following tactics, often used in combination, can amplify the impact of disinformation and deception. Addressing these threats holistically is critical to achieving the protective goals of this legislation:

- **Microtargeting:** Leveraging detailed user data and exploiting algorithmic biases to deliver tailored messages that influence undecided or vulnerable populations.
- **Algorithmic Amplification and Suppression:** Employing bots, coordinated inauthentic behavior, and engagement manipulation to amplify divisive content, elevate fringe narratives, suppress credible sources, or distort information ecosystems.
- **Information Laundering:** Disseminating disinformation through fake think tanks, pseudo-news outlets, or fabricated research to provide false content with an appearance of legitimacy and authority.
- **False Attribution and Identity Spoofing:** Using hacked accounts, impostor websites, or AI-generated personas to impersonate public figures, candidates, journalists, or trusted community leaders, thereby undermining credibility and trust.
- **Geofenced Misinformation Campaigns:** Deploying localized misinformation aimed at specific demographics or electoral districts, such as voter suppression targeting minority communities, using mobile ADTECH to deliver disinformation within defined geographic zones, including polling places or political events.

- **Dark Social Channels:** Utilizing encrypted or closed platforms such as WhatsApp, Signal, and Telegram to spread misinformation in ways that evade detection and moderation by traditional content-monitoring systems.
- **Synthetic or Inauthentic Engagement:** Creating the illusion of widespread support or controversy through bots, fake followers, and automated comment farms. These tactics exploit psychological phenomena like the Asch Conformity Effect to shape perceptions of public opinion.
- **Crowdturfing and Paid Influence Campaigns:** Orchestrating coordinated campaigns using compensated influencers or real users who promote narratives without disclosure, blurring the lines between organic opinion and paid propaganda.
- **Digital Voter Suppression:** Spreading false or misleading information about voting dates, eligibility, polling locations, or procedures, sometimes using AI-generated or spoofed communications that mimic official election authorities.