New Hampshire Committee on Commerce and Consumer Affairs

January 13, 2026

Dear Chairman Hunt, Vice Chair Potucek, and Members of the Committee,

Thank you for the opportunity to submit testimony on HB 1589, the proposed Digital Choice Act. While the bill is motivated by understandable concerns about user autonomy and platform power, I urge the Committee to reject this legislation. In practice, HB 1589 would undermine user privacy, weaken cybersecurity, entrench dominant firms, chill innovation, and impose a state-level regulatory regime that is technically unworkable and constitutionally suspect.

This bill implements government mandates overriding user choice, market competition, and technological evolution.

I. Mandated Interoperability Creates Severe Privacy Risks

HB 1589 attempts to frame interoperability as a means of empowering users. However, the bill requires companies to disclose highly sensitive user data, including social graphs, metadata, and behavioral information, to third parties through mandatory interfaces.

The definition of “personal data” in the bill is extraordinarily broad, including not only content and profiles, but metadata and relational references “sufficient to maintain associations among data elements.” That effectively means the architecture of a person’s online relationships and behaviors must be made portable and accessible to external entities.

This creates at least four serious privacy problems:

1. Attack surface expansion

Every required interoperability interface becomes a new attack vector. Even if a large platform invests heavily in security, the weakest linked third party becomes the vulnerability. The bill explicitly allows third parties to access and store this data, yet places no meaningful standards or enforcement mechanism on those third parties beyond vague obligations to “reasonably secure” data.

2. Consent becomes illusory

The bill requires “user consent,” but in practice, users already struggle to understand complex permissions. Interoperability dramatically multiplies the number of actors handling their data, making informed consent functionally impossible. A user might trust Platform A but unknowingly expose their data to Platform D, E, and F down the chain.

3. Re-identification risks explode

Even if individual data fields appear innocuous, social graph data is among the most powerful tools for re-identification. Academic research consistently shows that anonymized graph data can be trivially deanonymized when combined with auxiliary datasets. This bill forces companies to systematize and export exactly the kinds of datasets that are hardest to protect.

4. Collateral exposure of other users

A social graph of a user isn't just about that sole individual. It inherently contains information about other people, such as their connections, interactions, and behaviors. HB 1589 pretends this can be cleanly separated; in reality, it cannot. One user's "consent" functionally exposes others who never agreed to participate.

This proposed legislation does not strengthen privacy. It commoditizes and disperses sensitive personal data in ways that increase the likelihood of abuse, breach, and exploitation.

II. The Technical Mandates Are Unrealistic and Likely Unworkable

HB 1589 attempts to legislate software architecture. That rarely ends well.

The bill requires:

- Use of an "open protocol"
- Continuous, real-time data sharing
- Non-discriminatory access to interoperability interfaces
- Complete documentation disclosure
- Ongoing maintenance of compatibility with competing services

These requirements assume that social media services are modular utilities. They are not. They are highly complex, continuously evolving systems with tightly integrated design choices. Forcing architectural uniformity across platforms is not "neutral infrastructure policy". It's the government engaging in platform design.

Several technical issues arise:

1. Open protocol standardization freezes innovation

Protocols ossify. Once codified in regulation, they become difficult to change. Innovation shifts from improving user experience to complying with the mandated interface. Startups must build around regulatory compatibility rather than user value.

2. Real-time interoperability is enormously complex and costly

Maintaining continuous synchronization of dynamic social graphs across heterogeneous systems introduces synchronization errors, scaling challenges, and security vulnerabilities. These costs disproportionately harm smaller entrants, the very actors this bill claims to help.

3. Documentation disclosure risks exposing security-sensitive architecture

Although the bill excludes trade secrets in theory, in practice, robust documentation of interoperability interfaces can expose system structure in ways that materially assist malicious actors. This is a well-known tension in cybersecurity: transparency is valuable, but forced transparency at architectural boundaries can be dangerous.

4. State-level technical mandates fragment the internet

If New Hampshire adopts one interpretation of “acceptable protocols” and California adopts another, platforms will either withdraw services, limit features, or build lowest-common-denominator compliance nationwide. That harms users everywhere.

III. **This Bill Entrenches Dominant Firms and Harms Competition**

Ironically, interoperability mandates often benefit the largest incumbents.

Large firms have:

- Teams of compliance engineers
- Dedicated regulatory counsel
- Infrastructure budgets in the billions
- Capacity to absorb legal uncertainty

Small competitors do not.

A startup building a new social product would, under this bill, be required from day one to:

- Implement complex interoperability layers
- Support undefined open protocols
- Manage compliance risk with Attorney General rulemaking
- Defend against enforcement ambiguity
- This is a barrier to entry, not a doorway.

Moreover, dominant firms are best positioned to influence the “open protocols” the Attorney General recognizes, effectively steering regulation toward standards that favor their existing architectures. This is how regulatory capture works—not in theory, but in practice.

True competition arises when firms are free to differentiate on design, privacy model, content moderation approach, and technical architecture. This bill pushes toward enforced uniformity.

IV. **Market Solutions Already Exist—and Are Working**

The bill's legislative findings assert that companies "have demonstrated a pattern of restricting interoperability." But that ignores the flourishing ecosystem of voluntary data portability tools, APIs, integrations, and user-controlled export mechanisms that already exist.

We have seen:

- Data export tools (e.g., Takeout-style downloads)
- Third-party publishing tools
- Cross-posting services
- Decentralized protocols (like ActivityPub and others)
- User-driven migration between platforms

When users demand portability, companies respond because competition works.

Mandating one model of interoperability risks freezing today's debates into law tomorrow, crowding out emergent, potentially superior solutions.

V. **The Bill Raises Serious Constitutional and Federalism Concerns**

HB 1589 also raises potential constitutional issues.

1. Dormant Commerce Clause

This law would regulate national and global platforms based on the residency of New Hampshire users, effectively projecting New Hampshire's regulatory regime beyond its borders. Courts have repeatedly struck down state laws that attempt to impose internet-wide design mandates.

2. Compelled speech and editorial discretion

Interoperability requirements may interfere with platforms' ability to curate, structure, and moderate content according to their own policies. That raises serious First Amendment questions that this bill does not address.

VI. **The Fiscal Note Underscores the Bill's Practical Deficiencies**

The legislation's fiscal note admits that the bill will require new staff, including specialized technical expertise, but provides no funding and no clear estimate of scope. That is a red flag.

If we cannot accurately estimate the expenses needed to acquire the expertise required to oversee these systems, it strongly suggests the legislature should not attempt to regulate them through statutory mandate.

Conclusion

HB 1589 is well-intentioned but deeply flawed. It:

- Weakens privacy rather than strengthening it
- Increases security risks
- Imposes rigid technical mandates on dynamic systems
- Raises barriers to entry for startups
- Advantages incumbents
- Invites constitutional challenges
- Expands state regulatory power into domains better governed by innovation and competition

Digital choice is best preserved through competition, consumer empowerment, and technological freedom.

For these reasons, I respectfully urge the Committee to reject HB 1589.

Thanks,

James Czerniawski

Head of Emerging Technology Policy

Consumer Choice Center