Why Mandating Social Graph Interoperability Is Risky: Written Testimony on HB 1589

By Will Rinehart[1]

Introduction

I am writing to voice concerns about the Digital Choice Act.[2] In my professional capacity, I have testified before the Senate on data ownership, explored the technical problems in trying to change social media technology through regulation, and written extensively about interoperability mandates.[3] While the Act is framed as innocuous, what is being considered is one of the most complex, risky, and least tested forms of interoperability.

As currently written, the Act would require social media companies to share a user's social connections with other users and entities, their profile, comments, reactions, mentions, reposts, shares, and other engagements, as well as the "relational references sufficient to maintain the associations among" them. Maintaining these associations would likely mean that a social media platform like Facebook would be required to offer up the ordering, threading, and nesting of comments; mentions and tags connecting users across content objects; timestamps, visibility settings (public, friends-only, group-limited); group or page membership contexts; and even engagement metrics that determine how interactions are interpreted downstream.

In practice, if you and I were friends on Facebook and I decided to use an interoperable service, all of your comments would be included in the data stream. In other words, implementing interoperability for social graph data would require violating the privacy of users who never consented to data transfers in the first place.

As the following testimony explains, four problems stand out:

- The Digital Choice Act violates core tenets of privacy and would codify the same data-sharing architecture that enabled Cambridge Analytica.
- As written, the bill contradicts itself. It requires "continuous, real-time" data sharing while limiting that sharing to "reasonable and proportionate thresholds." Real-time federation and periodic data exports are fundamentally different systems with different privacy implications and different technical requirements.

---

[1] The American Enterprise Institute (AEI) is a nonpartisan, nonprofit, 501(c)(3) educational organization and does not take institutional positions on any issues. The views expressed in this testimony are those of the authors. This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in developing associated documents without attribution.

[2] New Hampshire General Court. (2025). *Digital Choice Act* (HB 1589). https://gc.nh.gov/bill_status/pdf.aspx?id=23963&q=billVersion

[3] Rinehart, W. (2019). *Data ownership: Exploring implications for data privacy rights and data valuation*. https://www.banking.senate.gov/hearings/data-ownership-exploring-implications-for-data-privacy-rights-and-data-valuation; Rinehart, W. (2018). *Breaking up tech means breaking up technology and teams*. American Action Forum. https://www.americanactionforum.org/insight/breaking-up-tech-means-breaking-up-technology-and-teams ; Rinehart, W. (2017). *The Social Graph Portability Act doesn't take tech seriously—and that's worrying*. Tech Policy Corner. https://techpolicycorner.org/the-social-graph-portability-act-doesnt-take-tech-seriously-and-that-s-worrying-63c7259a6fec

- The hard questions are left to rulemaking. The Act assumes that open protocols can support secure, abuse-resistant social networking across various platforms, but it doesn't specify minimum security standards or establish liability rules when data is breached or misused after leaving the originating platform.
- Finally, economic research suggests that interoperability is just as likely to entrench dominant platforms as to discipline them by encouraging hesitation, strategic incumbent responses, and partial exit rather than real competition.

The Privacy Implications of An Interoperability Mandate

The Digital Choice Act begins with three findings:

- An individual has a right to control and move the individual's own personal data, including social interactions online;
- Companies have demonstrated a pattern of restricting the interoperability of content, preventing users from easily sharing posts and interactions across different platforms; and
- The state should ensure that individuals have the right to access a complete personal data record from social media platforms.

These premises are intuitively appealing, but they rest on contested assumptions about the nature of personal data.

For one, the vast majority of data generated over the last several years is not produced independently. It exists due to structured interactions with specific platforms. If Google did not exist, there would be no search query data. If Facebook did not exist, there would be no social graph data. These datasets are co-created by users and platforms, a product of design choices that allow interactions to be possible in the first place. Treating this information as a freestanding personal asset obscures the extent to which the data is inseparable from the infrastructure that gives it meaning.

Second, companies do not uniformly restrict interoperability or prevent users from sharing content across platforms. Interoperability is an expansive term that can reference a range of technical arrangements like data portability and federation. Data portability refers to a user's ability to export profile data, posts, photos, or messages to another service. Typically, the data is exported as a zip file that can be easily read by another service. Federation, by contrast, allows users on different platforms to interact directly with one another in real time, often through shared protocols.

In practice, many major platforms already support meaningful forms of data portability. Initiatives like the Data Transfer Project enable users to move data directly between participating services without intermediaries, undermining the claim that platforms categorically lock users in. For example, Meta's Threads service has publicly committed to adopting open federation standards, allowing users to interact across services built on compatible protocols. Even where portability is imperfect or incomplete, it reflects tradeoffs among privacy, security, and technical feasibility, not a blanket refusal to enable user choice. Treating all resistance to full federation as anticompetitive obstruction collapses important technical and normative distinctions. More importantly, it risks mandating one particular vision of social networking under the banner of user choice.

Facebook's experience with open protocols is instructive precisely because it demonstrates how well-intentioned interoperability can collide with privacy and security realities. Facebook launched Version 1.0 of the Graph API in April 2010, then deprecated it in April 2014, finally closing the API in April 2015. The Graph API was revolutionary when it first launched, as it allowed for easy transfer of likes, connections, locations, and updates, much like what the Digital Choice Act seeks to enable today.

But it was the ease of communication that eventually led to its sunset. As was explained at Facebook's developer conference in 2014:

> We've heard from people that they are worried about sharing information with apps, and they want more control over their data. We are giving people more control over these experiences so they can be confident pressing the blue button.[4]

It is now clear that the Cambridge Analytica scandal was a predictable consequence of the Graph API's original permission structure. Cambridge Analytica obtained data through a researcher's quiz application, which collected not only the data of participating users but also extensive information about their friends. Secondary data sharing was possible precisely because the API allowed friend data to be accessed with minimal friction and limited downstream oversight. In practice, the Digital Choice Act would be implementing this scheme on every social media platform.

But the Digital Choice Act goes much further than what Cambridge Analytica was allowed to collect. That's because it treats relational network data as something users can port and share, beyond a mandate to share likes, reposts, and comments. In fact, the Act includes at least three separate mandates:

- Data portability (358-A:16) — Users can download their personal data in a portable format.
- Real-time federation (358-A:17.I.a) — Companies must let users "share a common set of their current social graph... between the social media services they designate" with continuous, real-time data sharing.
- Third-party access (358-A:17.I.b) — Third parties can access and get notifications about new social graph data with user permission.

But there is an inherent conflict in the way the bill is written. The requirement for "continuous, real-time" data sharing (358-A:17.III.b) is limited by "reasonable and proportionate thresholds" (358-A:17.III.c) on frequency. As written, then, the bill mandates both a federation protocol and a data export requirement, which are two different technical architectures.

Assuming that the bill is requiring continuous, real-time data sharing of the social graph through open protocols, it is choosing to implement one of the most complex, risky, and least tested forms of interoperability, without acknowledging the tradeoffs involved. The primary tradeoff lies in privacy.

Most privacy experts subscribe to Helen Nissenbaum's concept of privacy.[5] Privacy isn't about secrecy. It's about ensuring that information flows align with the norms of a given context. When we post on a social network, we do so with the understanding that our audience is limited to that

---

[4] Meta. (2014). *F8 2014: Stability for developers & more control for people in apps*. Meta Newsroom. https://about.fb.com/news/2014/04/f8-2014-stability-for-developers-and-more-control-for-people-in-apps/

[5] Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–157.

platform and its users. If the law compels a platform to transmit comments and other interactions to an entirely different service, the original context and expectations get upended. Such a law would be mandated context collapse.[6]

The carve-out excluding private messages is certainly a step in the right direction, but even if a user's comment is publicly visible on Facebook, for example, that doesn't necessarily mean they agree to have it shared externally. Public on one site isn't the same as public everywhere. A regulatory mandate that treats all platform interactions as fair game, unless explicitly flagged private, undermines contextual integrity and norms.

Not only does the Act violate a core tenet of privacy, but it also leaves open a raft of important technical questions for the rulemaking process. The Act assumes that royalty-free, patent-unencumbered protocols can support secure, abuse-resistant, large-scale social networking across heterogeneous platforms. Critically, the law does not specify minimum security standards or provide a liability framework for breaches or misuse once data leaves the originating platform. It goes without saying that this exact setup drove the case against Facebook over its sharing of data with Cambridge Analytica, leading to a $5 billion fine. It also relies heavily on downstream actors to comply with purpose limitations. It's for all of these important details that policymakers elsewhere have been hesitant to mandate interoperability protocols.

The Economics of An Interoperability Mandate

A substantial portion of the value of a social network comes in the value that users garner from their connections. Aral et al. estimate 20–34% of that value is due to local network effects, which is the direct value of being connected to specific friends or contacts.[7] Naturally, it is argued that making networks interoperable could unlock that value for competitors and consumers by reducing lock-in and encouraging competition on the merits. While the intuition is appealing, it rests on strong assumptions about how users and platforms actually respond to interoperability mandates, which might not hold in complex markets.

Research by Emanuele Giovannetti and Paolo Siciliani complicates the standard case for interoperability.[8] When users face different switching costs for each platform, which is almost always the case, mandates for interoperability can trigger incumbents to respond strategically, improving terms just enough to retain marginal users while also squeezing entrants before they can reach scale. In other words, the Act might trigger more aggressive incumbent behavior that discourages entry and shrinks the market share of entrants, even as switching becomes cheaper in theory.

Biglaiser, Crémer, and Veiga also uncovered counterintuitive results in their modeling of interoperability.[9] Their work shows incumbency advantage can arise even in the absence of

---

[6] Wikipedia. (n.d.). *Context collapse*. In *Wikipedia*. Retrieved January 13, 2026, from https://en.wikipedia.org/wiki/Context_collapse

[7] Aral, S., Benzell, S. G., Collis, A., & Nicolaides, C. (2025). *Measuring social media network effects*. arXiv. https://arxiv.org/abs/2507.04545

[8] Giovannetti, E., & Siciliani, P. (2023). Platform competition and incumbency advantage under heterogeneous lock-in effects. *Information Economics and Policy*, *63*, Article 101031. https://doi.org/10.1016/j.infoecopol.2023.101031

[9] Biglaiser, G., Crémer, J., & Veiga, A. (2022). Should I stay or should I go? Migrating away from an incumbent platform. *The RAND Journal of Economics*, *53*(3), 453–483. https://doi.org/10.1111/1756-2171.12418

switching costs, driven purely by users' strategic delay in migrating. When platform value depends on who else has moved, users rationally prefer to wait for others to go first, even when collective migration would leave everyone better off. Paradoxically, offering users more opportunities to migrate can make migration less likely. The option to wait dulls the urgency to move. The coordination never materializes, critical mass is never reached, and the incumbent remains dominant despite the presence of a superior alternative.

Both papers directly challenge the logic underlying social-graph interoperability mandates. In one plausible scenario, creating an environment that facilitates user exit might increase incumbency advantage by encouraging hesitation. Or a mandate might precipitate actions that entrench dominant platforms rather than disciplining them, keeping users tethered to incumbents under the appearance of choice. On top of this, in one of the few research papers that actually asked platform engineers what they thought of ported data, the "interviewees struggled to come up with new, competitive products they could build from, or meaningfully grow with, ported Facebook data."[10]

Interoperability may move data, but it might not necessarily move users or competitive advantage.

The Bottom Line

Understandably, the Digital Choice Act is motivated by concerns about user control and platform power, but its core remedy is misaligned with both the technical realities of social media and the economics of platform competition. By mandating deep interoperability of the social graph, the Act risks violating contextual privacy norms, exposing non-consenting users' data, and creating security obligations that are poorly specified and difficult to enforce. At the same time, economic research suggests that such mandates might not deliver the competitive benefits their proponents promise. Policymakers should be aware that the bill sounds great in theory, but may not deliver on its promises.

[10] Nicholas, G., & Weinberg, M. (2019). *Data portability and platform competition: Is user data exported from Facebook actually useful to competitors?* Engelberg Center on Innovation Law & Policy, NYU School of Law. https://www.law.nyu.edu/sites/default/files/Data%20Portability%20and%20Platform%20Competition%20-%20Is%20User%20Data%20Exported%20From%20Facebook%20Actually%20Useful%20to%20Competitors.pdf