

To: Minnesota House Committee on Judiciary Finance and Civil Law

Date: March 12, 2026

RE: Strong Opposition to H.F. 4081 – Testimony Regarding Data Privacy and Civil Law Provisions

Dear Chair, Co-Chair and Members of the Committee,

I am writing as a Minnesota property owner and a career cybersecurity professional to express my firm opposition to H.F. 4081. My testimony is focused strictly on the provisions within this committee's jurisdiction regarding data privacy and civil law: Article 1, Section 2, Subdivision 6 and Article 2, Section 1. I offer this perspective having worked in the Information Technology and Cybersecurity fields for 24 years across non-profit, private sector, and military settings. I hold a Master of Science in IT with concentrations in Information Assurance and Information Systems Security, a Bachelor of Science in IT Management, and am an ISACA Certified Data Privacy Solutions Engineer. Additionally, I hold CompTIA's Cybersecurity Analyst, Security+, Security Analytics Professional, and Secure Cloud Professional certifications, amongst others. From my professional vantage point, the data architecture proposed in this bill represents a catastrophic risk to the privacy and safety of Minnesota citizens.

The "Private Data" Fallacy and the 2026 BCA Data Breach

Article 1, Section 2, Subd. 6 classifies certification data as "private data on individuals." However, labeling a registry "private" under the **Minnesota Government Data Practices Act (MGDPA)** is a superficial safeguard that fails to account for state-level technical failures.

As a matter of record, in **early 2026**, the **Minnesota Bureau of Criminal Apprehension (BCA)**—the very agency H.F. 4081 tasks with managing this sensitive database—suffered a catastrophic data exposure. For nearly 30 days, private records were accessible on a public-facing website due to a technical misconfiguration. This real-world failure proves that the state cannot guarantee the security of a centralized "target list" of residences where high-value property is stored. Under the MGDPA, "private data" remains accessible to any government employee with a broadly defined "work assignment," exponentially increasing the risk of unauthorized leaks or political weaponization.

Constitutional Infringement and Legal Precedent

The data collection and certification requirements in **Article 2, Section 1** facilitate a regulatory scheme that directly conflicts with the U.S. Constitution and established Supreme Court precedent:

- **The Second Amendment Privacy Right:** National litigation, such as **SAF v. SIG SAUER (2026)**, is currently establishing that the Second Amendment includes an inherent right to **informational privacy**. Compelling citizens to register their identities to exercise a fundamental right creates a "chilling effect" that discourages lawful activity.
- **Compelled Disclosure:** Compelling citizens to register their identities to exercise a fundamental right creates a "chilling effect" that discourages lawful activity.

- **The "History and Tradition" Test:** Per **NYSRPA v. Bruen (2022)**, any firearm regulation must be consistent with the Nation's historical tradition. There is no 18th or 19th-century historical analogue for a mandatory, state-wide registry of commonly owned firearms, making the data collection in this bill constitutionally suspect.
- **Fourth Amendment:** The requirement for the BCA to adopt regulations on "safe and secure storage" and the subsequent certification of such storage implies a level of government oversight that infringes upon the "right of the people to be secure in their houses."
- **Due Process and Civil Law Concerns:** This bill allows for the denial of certification based on a "substantial likelihood" that a person is a danger. This standard is dangerously vague and grants law enforcement near-total discretion to suppress a constitutional right without the rigorous due process required for the deprivation of liberty or property.
- **State Overreach:** In **State v. Vagle (2025)**, the Minnesota Supreme Court cautioned against the state creating independent identification and regulatory regimes that lack federal alignment. H.F. 4081 ignores this by creating an invasive, state-specific certification system.

Conclusion

H.F. 4081 places an unconstitutional and technically unfeasible burden on the privacy of Minnesota citizens. The creation of a state-managed database—already proven vulnerable to exposure—is a significant overreach that invites both criminal exploitation and civil rights litigation. I urge this committee to reject the data privacy and civil law frameworks established in this bill.

Respectfully,

Michael Babcock
Saint Paul, MN 55106

Joel Ostmo
13611 Forestview Lane N.
March 13, 2026

The Honorable Rep. Tina Liebling
Judiciary Finance and Civil Law Committee
Minnesota House of Representatives
Saint Paul, MN 55155

RE: Opposition to HF 4081 – Data Privacy Concerns (Art. 1, Sec. 2 & Art. 2, Sec. 1)

Dear Chair Liebling and Members of the Committee,

I am writing to express my opposition to the data privacy provisions contained within **HF 4081**, specifically **Article 1, Section 2, Subdivision 6** and **Article 2, Section 1**.

While this bill seeks to regulate firearms, it simultaneously creates a massive new state database of private citizens. My concerns regarding these sections are as follows:

1. **Mass Data Collection (Art. 1, Sec. 2, Subd. 6):** This provision requires the Commissioner of Public Safety to maintain a permanent record of "assault weapon" certifications. This essentially creates a state-run registry of law-abiding citizens. History has shown that centralized government databases are vulnerable to cyberattacks and accidental leaks, which would put the safety and physical security of thousands of Minnesotans at risk.
2. **Inadequate Privacy Protections (Art. 2, Sec. 1):** While the bill classifies certain data as "private," Article 2, Section 1 provides broad exceptions for sharing this information with other law enforcement agencies and potentially other government entities. This "mission creep" turns private ownership data into a tool for state-wide surveillance of citizens who have committed no crime.

3. **Government Overreach:** The state should not be in the business of collecting and storing the digital "fingerprints" of constitutional rights-holders. The privacy risks far outweigh any purported public safety benefit.

I urge the committee to reject these intrusive data collection mandates and **vote NO** on HF 4081.

Sincerely,

Joel Ostmo



House Judiciary Finance & Civil Law
March 15, 2026

Re: Written Testimony Opposing HF4081

Madam Chair and Members of the Committee,

On behalf of the Minnesota Gun Owners Caucus and our members across the state, we submit this written testimony regarding HF4081.

First and foremost, we wish to make clear that **we oppose HF4081 in its entirety**. The bill proposes sweeping restrictions on commonly owned firearms and raises significant constitutional, policy, and practical concerns. For these reasons, we strongly believe the bill should not move forward.

We also believe it is important to note the procedural context in which this bill has arrived before this committee.

Earlier this session, a substantially similar proposal failed to advance from the House Public Safety Committee after a tie vote. Rather than allowing the committee's decision to stand, the bill author has introduced a new bill referred to this committee, effectively **bypassing the tied vote in the Public Safety Committee**.

While we recognize that bill referrals are ultimately within the authority of House leadership, this maneuver raises serious concerns about circumventing the normal committee process and undermines the legislature's credibility.

That said, we understand the committee has requested testimony specifically on provisions within its jurisdiction concerning **data privacy**, including **Article 1, Section 2, Subdivision 6**, and **Article 2, Section 1**.

With respect to those provisions, the bill classifies certain data relating to firearm ownership and certification as **private data on individuals** under Minnesota's data practices framework. In general, we agree that **personal information related to lawful firearm ownership should not be public data**. Firearm ownership records are sensitive personal information, and treating such information as private is consistent with longstanding public safety and privacy considerations.

However, while classifying such data as private is the correct approach to protecting individual privacy, **that limited point does not mitigate the broader concerns raised by the bill as a whole**.

HF4081 would impose sweeping prohibitions affecting commonly owned firearms owned by law-abiding Minnesotans. The Minnesota Gun Owners Caucus firmly believes this legislation represents an unjustified infringement on the constitutional right to keep and bear arms and would create significant legal and practical problems if enacted.

For these reasons, **we respectfully urge the committee to vote no and prevent HF4081 from advancing**.

Thank you for your consideration.

Sincerely,

Bryan Strawser
Chair

Anna Leamy
Director, Government Relations & Advocacy