

January 19, 2026

VIA ELECTRONIC SUBMISSION

House Committee on Commerce and Economic Development
Vermont State House
115 State St, Montpelier, VT 05633
Attn: Autumn Crabtree [Autumn.Crabtree@vtleg.gov]

RE: Written Testimony by Optery, Inc. with Respect to H.211

Dear Chair and Members of the Committee,

As General Counsel for Optery, Inc., I am writing to provide formal comments and proposed statutory revisions to H.211. Optery is the leading platform for automated personal data removal, unique in the privacy ecosystem for providing *verifiable results*. While other services provide simple status dashboards or static PDF files that are updated quarterly, Optery provides consumers with realtime status updates and free exposure scans to see where their personal data is published on the internet and actual screenshot evidence of their data being removed from data brokers.

Optery's technology provides a critical, nationwide privacy solution in our increasingly mobile society, working across state lines to support personal data removal for individuals whose digital footprints span multiple states over time. As the creator of the world's largest open-source directory of data brokers on [GitHub](#), our experience at the front lines of privacy advocacy has culminated in the development of a private-sector platform comparable to the DROP system. The Optery platform streamlines consumer efforts while allowing data brokers to receive and respond to requests in bulk.

Optery is pleased to see Vermont advancing its Delete Act. We believe that the prevention of "verification laundering" and the proper validation of authorized agents can protect against industry non-compliance through technical and operational loopholes, and we provide the following comments to support the strengthening of H.211:

1. Ending "Verification Laundering" with a Data Matching Catalog

A primary hurdle to effective deletion is the arbitrary "black box" of how data brokers match requests. Data brokers frequently use "unverifiable request" loopholes to ignore removals and often demand sensitive information, such as Social Security Numbers or government IDs, that they did not previously possess. A 2025 [University of California, Irvine \(UCI\) study](#) found that over 40% of registered data brokers fail to respond to requests, and many "paradoxically" create new privacy risks by harvesting new data during the verification process.

Optery maintains extensive documentation of the opt out processes for hundreds of data brokers, and publishes some of its documentation publicly in the form of [175+ manual opt-out](#)

[guides](#) that walk consumers through data broker opt-out and deletion forms, but these forms often collect *more* than what is strictly necessary to match a consumer record without explaining why. Vermont must mandate transparency regarding what is actually required for a data broker to reasonably identify and match a consumer record.

Proposed Definition for § 2430:

“Data Matching Catalog” means a public-facing document, updated in real-time or upon any change to data processing practices, published by a data broker that lists the specific, individual personal data elements or identifiers the data broker possesses, processes, or has access to—including data held by service providers, parent companies, or subsidiaries—that are used, or are technically capable of being used, to match, link, or identify a consumer to a record for the purpose of fulfilling a disclosure, opt-out, or deletion request.

This includes, but is not limited to: (A) Direct identifiers such as name, physical address, email address, and telephone number; (B) Unique persistent identifiers such as IP addresses, cookie IDs, and mobile advertising IDs; and (C) Inferred or probabilistic identifiers used by the broker to associate disparate data points with a single natural person.

A data broker shall not require a consumer to provide any data element for the purpose of matching or verification that is not explicitly listed in its Data Matching Catalog.

Proposed Statutory Language for § 2446(a)(3):

Data Matching Catalog. Each registered data broker shall publish a “Data Matching Catalog” specifying the personal data elements it possesses—or has access to via a service provider or parent/subsidiary entity—that are used, or are technically capable of being used, to identify or link a consumer to a record.

(1) Verification Limitation: A data broker is prohibited from requiring any personal data element for the purposes of matching, identifying, or verifying a request that is (A) not listed in its Data Matching Catalog or (B) not already in its possession at the time of the request.

(2) Minimum Necessary Standard: To honor a request, a data broker shall require only the minimum personal data element(s) strictly necessary to achieve a probabilistic or deterministic match to the consumer record. A data broker may not require a consumer or their authorized agent to provide more data elements than the broker currently uses to uniquely identify a consumer in the ordinary course of its business.

(3) Conclusive Verification: If an authorized agent provides any of the data element(s) specified in the Data Matching Catalog, the match shall be deemed conclusively verified. The data broker shall not require further interaction with the

consumer, nor shall it require additional documentation (such as a notarized statement or government-issued identification) to validate the agent's authority, provided the agent has certified its authorization to the Secretary of State.

2. Standardizing Agent Accountability and Credentialing

The data broker industry sometimes attempts to discredit authorized agents to preserve the friction that keeps the sale of consumer personal data highly profitable. The solution is to establish a high bar for agent accountability that ensures they are legitimate, privacy-first actors.

Proposed Statutory Language for § 2446c:

Agent Accountability and Credentialing. *An authorized agent must certify to the Secretary of State that it (1) does not sell or share personal data it receives for the purpose of fulfilling consumer privacy rights requests, (2) maintains a verifiable point of contact, and (3) maintains auditable records of requests submitted and responses received, including evidence of removals or denials. In return, a data broker must accept requests from credentialed agents as legally binding and shall not attempt to verify the agent's authority on a per-request basis if a blanket authorization is on file.*

3. Preventing Government “Honeypots” and Surveillance

The push for centralized state-run “DROP” portals modeled after California creates the potential for multiple centralized honeypots of consumer identifiers. Public comments on the California system warn that such databases represent a [significant privacy threat](#) if breached.

Optery provides a nationwide private-sector alternative that meets the rigorous security and data handling standards required by its corporate, enterprise, and government customers. By utilizing accountable and vetted authorized agents, Vermont can support a technologically advanced consumer privacy ecosystem that achieves the state's goals without the government maintaining a massive, vulnerable database of its citizens' personal identifiers that may be costly or impractical to manage going forward.

4. Cutting Off Industry Loopholes: B2B Data and Verification Fatigue

We must sharply refute the following arguments presented by the data broker and advertising industries:

- **The “B2B Persona” Fallacy:** Data brokers that sell business contact information argue they should be exempt from deleting “professional” data, asserting that such information belongs to the employer rather than the individual. These B2B data brokers downplay the privacy implications as *de minimis*, equating the exposure of professional profiles to the triviality of losing a few business cards in a public space. In reality, professional or B2B personal data is frequently used for doxxing, harassment, phishing, and other social engineering techniques that result in widespread cybersecurity incidents and cause harm to businesses whose personnel are opted into those directories without their explicit

opt-in consent. Additionally, given how easy it is to link B2B personal data to an identified or identifiable individual consumer, H.211 must clarify that PII includes personal data that is reasonably linkable to a natural person in *any* capacity.

- **Direct Contact and “Verification Fatigue”:** In Optery’s experience, some data brokers attempt to circumvent authorized agents by contacting consumers directly. This practice confuses the public and induces “verification fatigue” due to a lack of standardized verification procedures across the data broker ecosystem. Optery believes this is a tactical maneuver designed to discourage consumers from exercising their rights while creating a false record of “unverified requests” to justify non-compliance.

Proposed Statutory Language for § 2430 or § 2446:

***Exclusive Correspondence.** If an authorized agent is designated, the data broker must correspond exclusively with that agent. Direct contact with the consumer to bypass the agent shall be considered an unfair and deceptive act under § 2453.*

Conclusion

By requiring a Data Matching Catalog that limits data collection to critical elements strictly necessary for matching a consumer record and establishing Agent Accountability standards, Vermont will create a functional “Right to be Forgotten” that is resilient to industry gamesmanship. We urge the Committee to adopt these amendments to protect the privacy and security of all Vermonters.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ambar Chavez', with a stylized, flowing script.

Ambar Chavez

General Counsel & VP, Legal
Optery, Inc.

Sources for Review

1. UCI Research on CCPA Non-Compliance (Nov 2025): <https://arxiv.org/abs/2506.21914v2>
2. Consumer Reports / EFF / EPIC Joint Comments (June 2024): [Joint Preliminary Comments on SB 362](#)
3. California DROP Public Comments: [Preliminary Comments on the Delete Act](#)
4. Optery Data Broker Directory (GitHub): <https://github.com/optery/optery-data-brokers-directory>

CC List:

Rep. Michael Marcotte (Chair): mmarcotte@leg.state.vt.us

Rep. Monique Priestley (Clerk): mpriestley@leg.state.vt.us

Rep. Edye Graning (Vice Chair): egraning@leg.state.vt.us