LEGAL REVIEW

The Legality of Person-Based Intent Data

A referenced review of the statutes, case law, enforcement actions, and industry frameworks that govern the licensing of person-level intent data into embedded products, prepared for the legal and compliance teams of Delivr.ai's embedded data customers.

Published · August 2026 **Scope** · United States (primary), EU/UK (transfer posture)

References · 103 sources: 102 verified public authorities and the Delivr.ai standard taxonomy build

This white paper is not legal advice. It is a factual survey of publicly available legal authorities, prepared to assist customers' counsel in evaluating person-based intent data licensing. It reflects authorities verified as of August 24, 2026. Several matters described here remain pending and will change. Every factual legal claim carries a numbered reference to its source, and no unverified claims are included. Consult your own counsel before relying on any statement in this document.

CONTENTS

SECTION 1

Executive summary

Person-based intent data is lawful to license and embed in the United States, provided the licensing program operates within a compliance perimeter that is now well established. That perimeter is defined not by a single statute but by a decade of FTC enforcement, the comprehensive privacy laws of more than nineteen states, data broker statutes, wiretap litigation over collection pixels, sensitive-inference rules, and federal transfer restrictions.

Six conclusions organize the analysis that follows.

- **Selling person-level behavioral data is not unlawful in itself, and in some settings it is constitutionally protected speech.** In *Sorrell v. IMS Health*, the Supreme Court held that the creation and dissemination of information, including the sale of person-identified records for marketing purposes, is expression protected by the First Amendment, and that the state may not burden it with content-based and speaker-based restrictions absent adequate justification.[102] Regulation therefore concentrates on how the data is collected (consent and notice), what it reveals (sensitive categories), and where it flows (downstream and cross-border controls).
- **The FTC's theory of harm requires three elements in combination:** person-linkable identifiers, sensitive inferences, and unrestricted downstream use. Every significant order since 2022, including Kochava, X-Mode, InMarket, Mobilewalla, Gravy Analytics, and Avast, rests on those three elements together.[1–13] A licensing program that verifies consent at collection, suppresses sensitive segments, and imposes enforceable downstream restrictions operates within the boundary those orders establish. A program lacking any of the three presents the fact pattern the orders were entered to address.
- **What is licensed matters as much as how it was collected.** Every browsing-data matter on the enforcement record involved the transmission of raw behavior to buyers. Avast sold the browsing histories themselves.[13] Healthline permitted advertising partners to receive the titles of the health articles a reader was viewing.[24] Kochava and the location brokers sold raw coordinate feeds.[1,5] Mobilewalla resold harvested bid requests.[9] Oracle's private settlement covered captured URLs and form text.[86] A taxonomy-score architecture licenses none of those artifacts. The underlying events are assessed inside the platform, and the licensed record is a score against a standard topic taxonomy, without URLs, page titles, or clickstream. That design difference distinguishes the central fact pattern of the raw-data cases. It does not remove the record from privacy law, because scores are inferences and inferences are regulated personal information,[19] but it determines which precedents actually describe the product.
- **Hashed emails are personal data.** The FTC has taken this position since 2012 and restated it in 2024. The CCPA's text covers persistent pseudonymous identifiers, and EU law reaches the same conclusion for any party with the means to re-identify.[17,18,19,52] A compliance posture premised on hashing as anonymization fails. A posture that treats hashed emails as pseudonymous personal information, handled under the applicable rules, is defensible.

- **Sensitive inference carries the highest exposure.** Intent topics that reveal health conditions, sexuality, religion, or precise location are regulated as sensitive data in California, Colorado, Connecticut, Washington, Nevada, and Maryland. Maryland prohibits their sale outright, with no consent exception, and Washington attaches a private right of action.[27,32,56] A compliant product excludes or gates sensitive-category topics. Delivr.ai's taxonomy carries a per-topic sensitivity classification so that these treatments attach to the topic record itself (Section 9.4).[103]
- **The licensor is accountable in both directions, and so are its customers.** FTC orders and case law hold data sellers responsible for their suppliers' consent failures and for their buyers' misuse.[8,87,88] California has imposed penalties for the absence of required contract clauses in data supply agreements, without any showing of downstream misuse.[25] Under current law, the license agreement is a component of the product itself. Embedded customers likewise inherit obligations rather than immunity: a customer embedding licensed person-level intent data becomes, in most states, a data recipient with its own opt-out, deletion, and contract duties, and, if it re-licenses the data, its own data broker registration duties.[34,40] Section 15 provides the working checklist.

Summary. The operative question for a compliance team is not whether intent data is legal in the abstract. It is whether the vendor's collection practices, identifier handling, sensitive-topic policy, opt-out infrastructure, and contract terms satisfy what the enforcement record now requires. This paper sets out that record so the comparison can be made provision by provision.

SECTION 2

What person-based intent data is, and what it is not

Definitions control the analysis. Nearly every legal rule discussed below turns on how data is collected, what identifier it is joined to, and what it can reveal.

Delivr.ai operates a deterministic identity resolution platform. A first-party pixel on a participating website observes a visit. The visitor's browser cookie or mobile advertising ID resolves deterministically, by exact graph match rather than statistical modeling, to a hashed email address (HEM), which links to a unified person profile. The platform uses no device fingerprinting and no probabilistic matching at any point in the chain. Intent is then scored per person: each individual's observed content consumption is compared against that person's own baseline, and deviations are scored across a standard taxonomy of intent topics comprising 59,070 active topics in the August 2026 build.[103] "Person-based intent" therefore means a person-level record, tied to an identified or identifiable individual, carrying topic-level scores derived from what that person read, watched, or researched.

One architectural fact frames the analysis throughout this paper: **the licensed record contains topic scores, not behavior.** The observed events, meaning the pages a person visited, the titles of those pages, and what was clicked or searched, are inputs assessed inside the platform, where content and frequency are evaluated against the standard taxonomy to produce each score. Those underlying events, URLs, and titles are not part of the licensed dataset and are not exposed to customers. Where this paper discusses cases concerning the sale of browsing histories, article titles, or raw location feeds, it is describing products that transmitted the behavior itself. That is a different artifact from an abstracted topic score, and the distinction is drawn explicitly where it matters. The converse is stated with equal clarity: the abstraction provides no protection where the law regulates the inference itself. Sale definitions, opt-out rights, data broker statutes, and sensitive-inference rules all reach scored topics directly (Sections 6, 7, and 9).

The taxonomy is itself a governance instrument rather than a topic list alone. Each topic carries per-topic metadata alongside its category hierarchy, including a dedicated sensitivity classification field, so that topic-level treatment rules (suppression, gating, and state-specific exclusion) attach to the taxonomy record itself rather than to after-the-fact filtering.[103] Section 9.4 describes how that classification corresponds to the statutory sensitive-data categories.

"Embedded data customers" license this data to power features inside their own products, such as enrichment fields, scores, and audiences visible to their end users. In Delivr.ai's contract architecture this is a Tier 2 (Embedded Use) data-rights grant, positioned between Tier 1 internal use and Tier 3 white-label distribution. Each tier's obligations follow from the legal authorities discussed in this paper.

Three legal characterizations follow directly from that description, and each carries analytical weight.

- **The records are personal information.** They are keyed to persistent identifiers (HEMs, cookies, and MAIDs) that are linkable to individuals, which is the statutory definition of personal information under the CCPA and the operative test under the FTC Act and the GDPR.[19,17,52] Section 5 develops this point.
- **The scores are inferences, and inferences are regulated.** California's statute expressly includes "inferences drawn … to create a profile about a consumer reflecting the consumer's preferences … predispositions, behavior" within personal information, and the California Attorney General has concluded that internally generated inferences are disclosable to the consumer on request even where the underlying algorithm is a trade secret.[19,21]
- **Licensing the records is a "sale."** Under the CCPA and the majority state pattern, transferring personal information for monetary or other valuable consideration is a sale, and a transfer for cross-context behavioral advertising is a "share" regardless of consideration.[19] Enforcement has applied these definitions to the exchange of data for analytics services (Sephora) and to marketing cooperative arrangements (DoorDash). The label placed on the transaction does not control.[22,23]

> **What this product is not.** The analysis below repeatedly distinguishes practices in which Delivr.ai does not engage: device fingerprinting, probabilistic identity modeling, precise-location data feeds, bidstream harvesting, eligibility (credit, employment, or insurance) scoring, and, centrally, the licensing of raw behavior in any form. No browsing histories, no URL or article-title feeds, and no clickstream event streams leave the platform. Several of the enforcement actions cited in this paper turn on exactly those practices. Where that is the case, the distinction is stated expressly.

SECTION 3

The legal frame: no single statute, eight overlapping regimes

The United States has no omnibus federal privacy statute. The legality of licensing person-level intent data is instead governed by eight regimes that apply concurrently to the same record.

REGIME	WHAT IT GOVERNS	ENFORCER / PLAINTIFF	EXPOSURE
FTC Act § 5 unfairness/deception	Sale of linkable behavioral data, sensitive inferences, consent verification, downstream controls	FTC	High
State comprehensive privacy laws (CA, CO, CT, VA, TX, OR, MD, and twelve others)	Sale and sharing definitions, opt-outs and GPC, sensitive data consent, contract terms, inferences	State AGs, CPPA	High
Data broker statutes (CA Delete Act, VT, TX, OR, NJ Daniel's Law)	Registration, deletion mechanisms, covered-person takedowns	Regulators; private plaintiffs in NJ	High
Wiretap and pen-register statutes (CIPA, ECPA, state acts)	The collection layer: pixels, session capture, identifier acquisition	Class-action plaintiffs	High
Consumer health data acts (WA MHMDA, NV, CT)	Health inferences from any data, sale authorizations	WA: private right of action; NV/CT: AGs	High

REGIME	WHAT IT GOVERNS	ENFORCER / PLAINTIFF	EXPOSURE
Sectoral statutes (VPPA, FCRA, COPPA)	Video-derived signals, eligibility uses, children's data	Private plaintiffs (VPPA/FCRA), FTC	Medium
National-security transfer rules (PADFAA, DOJ 28 C.F.R. Part 202)	Data brokerage with foreign adversaries; onward-transfer clauses	FTC (civil penalties), DOJ NSD	High
EU/UK law (GDPR, ePrivacy)	Consent for tracking, special-category inference, profiling	DPAs, competition authorities, courts	High if EU persons in

Two structural doctrines constrain all eight of the regimes tabulated above. First, *Sorrell v. IMS Health* establishes that the sale and dissemination of data is protected speech, which constrains how far legislatures may go. It is the basis of the pending constitutional challenge to New Jersey's Daniel's Law.[102,41] Second, *Spokeo v. Robins* and *TransUnion v. Ramirez* limit private statutory suits in federal court to plaintiffs with concrete harm, and *TransUnion* specifically holds that dissemination to a third party is what renders a data-record injury concrete.[101,100] For a licensing business the doctrine has two consequences: it narrows plaintiff classes, and it makes each delivery of a record to an embedded customer the act capable of establishing standing.

SECTION 4

FTC enforcement: the data broker line of cases

Between 2022 and 2026, the FTC constructed, case by case, an effective rulebook for the sale of person-linkable behavioral data. The actions were brought under Section 5 of the FTC Act without any new statute, and they bind through consent orders and through the litigation risk the Kochava rulings established.

4.1 Kochava: the anchor litigation

A federal court has held that selling non-anonymized, readily linkable person-level data states a claim for unfair practices under Section 5 of the FTC Act, and that the invasion of privacy is itself a substantial injury under Section 5(n) without proof of any further harm. That is the holding of *FTC v. Kochava*, and it is the most directly applicable judicial authority in this area.[2]

The FTC sued the data broker Kochava in August 2022 for selling data feeds that matched mobile advertising IDs to timestamped locations, alleging that the data was person-linkable, that it could expose visits to reproductive health clinics, places of worship, and shelters, and that Kochava imposed effectively no restrictions on downstream use.[1] Judge Winmill denied the motion to dismiss the amended complaint in February 2024, and denied dismissal a second time in February 2025 after Kochava moved the broker business into a subsidiary.[2,3]

The complaint the court sustained was not limited to location, which is what makes the ruling relevant to intent data. It covered Kochava's "Database Graph" of person-level profiles containing up to 300 data points, including interests, behaviors, and political affiliation, together with audience segments sorted by web usage and religious affiliation. The court noted that the products included "Kochava's own inferences about consumers."

The case settled in May 2026 with a stipulated order that now serves as the FTC's compliance template. The order prohibits the sale of sensitive location data without affirmative express consent and requires a supplier assessment program verifying consent for all acquired data, incident reports to the FTC when a third party violates its contract, disclosure of purchaser names to consumers on request, a consent-withdrawal mechanism, and a retention and deletion schedule.[4]

4.2 The consent orders of 2024 and 2025

ACTION	DATA PRACTICE CHARGED	SIGNIFICANCE FOR A LICENSOR
X-Mode / Outlogic	Sold raw location tied to MAIDs; failed to verify supplier-app consent; built a	The first order banning the sale of sensitive location data. The seller answers both for its suppliers' consent failures and

ACTION	DATA PRACTICE CHARGED	SIGNIFICANCE FOR A LICENSOR
(Jan 2024)[5,6]	segment of visitors to specific medical facilities; provided "means and instrumentalities" for others' deception	for its buyers' capabilities. Building targeting segments from behavioral signals is independently actionable. The order requires supplier assessments within 30 days of any data-sharing agreement
InMarket (May 2024)[7,8]	Combined SDK location with other data into audience segments ("parents of preschoolers," "Christian church goers") without verified consent; retained data for five years	The prohibition reaches derived audience-categorization products, not only raw data, so abstraction alone is not a defense. The condemned segments encoded sensitive traits and rested on unverified collection. A derived product survives on the strength of its consent chain and its sensitive-category exclusions. Reliance on a supplier app's consent flow fails without verification and records
Mobilewalla (Dec 2024)[9,10]	Harvested RTB bid-request data beyond auction purposes (500M+ advertising IDs); sold segments built on sensitive traits (pregnancy, race of protest attendees)	The first action treating bidstream harvesting as an unfair practice, which constrains how intent signals may be sourced. The order requires written supplier certifications of authority to provide the data, and deletion instructions that extend to customers
Gravy Analytics / Venntel (Dec 2024)[11,12]	Operated purely as a reseller, collecting nothing itself; sold sensitive characteristics derived from location, including health decisions, political activity, and religious viewpoints	Reseller status does not insulate a seller. The FTC treats the inference layer as the regulated product. Customers who received data in the prior three years were required to be instructed to delete or de-identify it, demonstrating that licensed data can be recalled retroactively
Avast / Jumpshot (Feb 2024)[13]	Sold browsing histories of more than 100 million users with a persistent browser identifier; contracts permitted one buyer to join the data to identity "on an individual user basis"; $16.5M in redress	The leading precedent for web-content-consumption data, and the one a taxonomy-score model is designed to be distinguishable from. Avast transmitted the browsing histories themselves, site by site, with a persistent identifier, and its contracts permitted a buyer to rejoin the data to individuals. A product that licenses only topic scores transmits neither the

ACTION	DATA PRACTICE CHARGED	SIGNIFICANCE FOR A LICENSOR
		histories nor the titles. The order's other holdings remain applicable: person-level browsing signals reveal health, religion, politics, and finances; a pseudonymous identifier does not anonymize; and derived models built on unlawfully obtained data were ordered deleted
BetterHelp (2023)[14] / **GoodRx** (2023)[15]	Disclosed emails, IP addresses, and health-context data to advertising platforms; GoodRx was the first Health Breach Notification Rule action ($1.5M penalty)	Identifiers combined with behavioral context are treated as health data because of what the disclosure implies. Unauthorized ad-tech disclosure of identifiable health data is a reportable "breach"
General Motors / OnStar (Jan 2025, finalized Jan 2026)[16]	Collected driving-behavior telemetry through a misleading enrollment flow and sold it to consumer reporting agencies	The enforcement line continued across the change in administration: the action was voted out under Chair Khan and finalized under the Ferguson Commission. Behavioral telemetry, not only location, is within scope, and defective consent at collection invalidates every downstream license

Reading the orders as a compliance specification. Across the Kochava, X-Mode, InMarket, Mobilewalla, Gravy Analytics, Avast, and General Motors actions, the same architecture recurs: (1) provable, verified consent at collection; (2) no sensitive-category products; (3) written supplier certifications; (4) enforceable downstream use restrictions with breach reporting; (5) deletion that propagates to customers; and (6) retention schedules. Section 13 maps these onto license terms. Two further observations follow from the record. The orders do not prohibit non-sensitive, consent-sourced, contract-restricted audience and interest data, which remained lawful to sell in every one of these matters. And every one of these matters involved a seller that transmitted raw behavioral records, whether coordinate feeds, browsing histories, or bid requests, among its products. None involved a product limited to derived topic scores with the underlying behavior withheld.

SECTION 5

Identifiers: hashed emails are regulated personal data

The identity layer of an intent product depends on how the law treats hashed emails. The answer is settled: a HEM is pseudonymous personal information, and it is never "anonymous," for any party with the means to match it.

5.1 The US position

FTC staff stated in July 2024 that hashed identifiers, expressly including hashed emails, are not anonymous, because a hash is a persistent unique signature that tracks a person over time, and that the agency will treat claims that hashing anonymizes data as actionable misrepresentations.[17] The publication reaffirms the FTC's 2012 position that hashing common identifiers is trivially reversible and "vastly overrated as an 'anonymization' technique."[18] Enforcement practice is consistent with these statements. In BetterHelp, the transmission of hashed emails to Facebook was treated identically to the transmission of the emails themselves, because Facebook could match the hashes and learn who was seeking counseling.[14,17] In Mobilewalla and InMarket, the Commission treated persistent pseudonymous identifiers joined to behavioral data as identifiable consumer data and prohibited misrepresentation of the degree of de-identification.[9,7] The Kochava court likewise held that a dataset keyed on MAIDs that customers can re-identify states an unfairness claim.[2]

The CCPA reaches the same result by its plain text. Personal information includes "unique identifiers," defined as persistent identifiers that recognize a consumer or device over time and across services, and the statute enumerates cookies, mobile advertising identifiers, "unique pseudonym[s]," and "other forms of persistent or probabilistic identifiers."[19] Pseudonymized data remains personal information. Only data meeting the statutory de-identification standard is excluded.

5.2 The EU position and its limits

The CJEU's *Breyer* test makes an identifier personal data for any party with lawful and practicable means to re-identify it with the help of additional information.[52] A vendor operating a HEM-to-profile resolution graph always has those means, so the graph is personal data in the vendor's hands. In September 2025, the Court of Justice confirmed in *EDPS v. SRB* that pseudonymised data is not automatically personal data for every recipient. Where the recipient has no reasonable means of re-identification, the data may fall outside the GDPR for that recipient while remaining personal data for the controller.[53] The EDPB's Guidelines 01/2025 on pseudonymisation address the same subject.[54] For an identity-resolution product, the exemption is largely academic. The product being licensed is resolution capability, so a customer licensing that product acquires the means of identification, and the data is personal data in that customer's hands as well.

5.3 The counter-current

One federal statute has been construed in the opposite direction. In *Solomon v. Flipps Media* (2d Cir. 2025), the Second Circuit joined the Third and Ninth Circuits in holding that a Facebook ID accompanied by video titles, transmitted by a pixel, is not "personally identifiable information" under the VPPA, because an ordinary person, as opposed to a sophisticated technology company, could not identify the viewer from it.[55] That "ordinary person" standard construes one statute's term and does not extend to the FTC Act, the CCPA, or state privacy law, all of which apply linkability tests. It is relevant to calibrating VPPA class-action exposure (Section 10), not to the general status of hashed emails.

> **Practical rule.** HEM-keyed data should be described as "pseudonymous personal information," and never as "anonymous" or "anonymized," in marketing, contracts, and privacy notices alike. The FTC has stated that the misdescription is itself the violation.[17]

SECTION 6

State comprehensive privacy law: sale, sharing, and inferences

More than nineteen states now regulate the sale of personal data. Five features of these laws carry the analysis for intent data: broad sale definitions, the treatment of inferences as personal information, enforceable opt-out signals, sensitive-data consent requirements, and mandatory contract terms.

6.1 California: the template and the enforcement record

The CCPA, as amended by the CPRA, defines "sell" as communicating personal information for monetary or other valuable consideration, and "share" as any transfer for cross-context behavioral advertising. Personal information expressly includes inferences drawn to create a profile reflecting preferences, predispositions, and behavior, and "sensitive personal information" (including health, sex life, precise geolocation, and religion) carries a separate right to limit use.[19] The Attorney General has concluded that internally generated inferences are disclosable to the consumer on request notwithstanding trade-secret protection for the algorithm, so the intent scores themselves are subject to right-to-know requests.[21]

California's enforcement record maps directly onto an intent-data supply chain.

- **Sephora (2022, $1.2M):** permitting ad-tech and analytics vendors to collect visitor data in exchange for services is a "sale," and Global Privacy Control signals must be honored.[22]
- **DoorDash (2024, $375,000):** contributing customer data to a marketing cooperative in exchange for marketing opportunities is a sale. An exchange of data for data satisfies the consideration element.[23]
- **Healthline (2025, $1.55M, the largest CCPA settlement to date):** sharing readers' data with advertisers, including the titles of the health articles they read, violated the CCPA's purpose-limitation principle, and the judgment prohibits sharing article titles that reveal a possible diagnosis.[24] This is the closest existing enforcement analogue to intent data, and it is the clearest point at which the taxonomy-score distinction operates. Healthline transmitted the article titles themselves to ad-tech partners. A topic score discloses neither the title nor the page a person read. What survives the distinction is that a health-topic score remains sensitive by implication, which is the subject of Section 9.
- **CPPA orders: Honda (2025, $632,500) and Todd Snyder (2025, $345,178):** opt-out mechanisms must operate without friction or identity verification, and Honda was fined in part for sharing personal information with ad-tech companies without producing contracts containing the CCPA's required terms.[25]

6.2 The other states in brief

STATE	KEY RULE FOR INTENT LICENSING	STATUS / ENFORCEMENT
Colorado[26,27]	Opt-outs for sale, targeted advertising, and profiling; the first state to make a universal opt-out signal (GPC) mandatory by rule; the AG's rules treat browsing-derived sensitive inferences as sensitive data (Section 9.1)	In force; universal opt-out mandatory since July 1, 2024; cure period expired January 1, 2025
Virginia[28]	The narrowest sale definition (monetary consideration only); opt-outs for targeted advertising, sale, and consequential profiling; opt-in consent for sensitive data	In force since January 1, 2023
Connecticut[29]	Broad (valuable-consideration) sale definition; mandatory opt-out preference signals since January 1, 2025; an active AG privacy unit that has issued cure notices on sale and targeted-advertising disclosures	In force; annual public enforcement reports
Texas[31]	Broad sale definition; scripted notices ("NOTICE: We may sell your sensitive personal data"); universal opt-out honored from January 1, 2025; no small-business exemption for sensitive-data sales	*Texas v. Allstate/Arity* (filed January 2025), the first suit under any state comprehensive privacy law, targets a data business that built and sold a person-level driving-behavior database sourced through third-party app SDKs. It is the closest litigation analogue to an intent-data supply chain[31]
Maryland[32]	The strictest regime: data minimization that consent cannot cure, and a prohibition, with no consent exception, on selling sensitive data (which includes use-based consumer health data, sexuality, religion, and immigration status)	Effective October 1, 2025; full enforcement since April 1, 2026

STATE	KEY RULE FOR INTENT LICENSING	STATUS / ENFORCEMENT
Oregon[33]	Consumers may demand a list of the specific third parties, not merely categories, that received their data. An intent vendor's customer list is therefore discoverable by any Oregon consumer whose record was licensed	In the DOJ's first six months: 110 complaints, with data brokers the largest category; a cure-notice sweep directed at brokers

Operational consequence. A compliant person-level intent product must (1) treat every license and every advertising distribution as a sale or share requiring notice and opt-out; (2) honor GPC and state universal opt-out signals within the data pipeline, not only on a website; (3) obtain opt-in consent for sensitive categories or suppress them; (4) exclude Maryland residents' sensitive-topic scores entirely; and (5) maintain per-recipient disclosure logs sufficient to answer Oregon-style access requests.

SECTION 7

Data broker registration and deletion regimes

A vendor licensing person-level data concerning consumers with whom it has no direct relationship is a "data broker" in every state that uses the term. An embedded customer that re-licenses the data meets the same definition.

7.1 California's Delete Act: registration and an operating deletion mechanism

The Delete Act requires annual registration with the CPPA by January 31, and it required the agency to build a single deletion mechanism (DROP), which opened to consumers on January 1, 2026. Since August 1, 2026, registered brokers must poll DROP at least every 45 days, delete matched consumers within 45 days, repeat the deletion every 45 days thereafter, and cease selling or sharing new information about those consumers. Independent compliance audits begin in 2028. Penalties are $200 per day for failure to register and $200 per deletion request per day for failure to process deletions, a figure that scales with the size of the database.[34] The agency's December 2025 enforcement advisory adds that every entity meeting the definition must register independently. Subsidiaries, trade names, and white-label brands may not rely on a parent company's registration.[35] The registration sweep is active. The CPPA fined Accurate Append, a data-append vendor whose business model is adjacent to intent licensing, $55,400 for late registration, alongside orders against National Public Data and Background Alert.[36]

7.2 Vermont, Texas, and Oregon

Vermont's 2018 law, the original template, requires annual registration and public disclosure of opt-out methods and breach history.[37] Texas Chapter 509 requires registration at $300 per year, a security program, and, notably for embedded models, public disclosure of whether the broker credentials its purchasers, with Attorney General penalties of up to $10,000 per twelve-month period.[38] Attorney General Paxton notified more than 100 unregistered companies within four months of the first deadline.[39] Oregon makes registration a precondition to collecting, selling, or licensing brokered personal data, and its "reasonably associable with a resident" definition reaches records keyed to hashed emails.[40]

7.3 New Jersey's Daniel's Law: liability without fault for missed takedowns

Daniel's Law permits covered persons (judges, police officers, prosecutors, and their household members) to demand removal of home addresses and unlisted telephone numbers, with liquidated damages of $1,000 per violation. The assignee Atlas Data Privacy Corp. sued approximately 150 data companies in 2024. In August 2026, answering a certified question from the Third Circuit, a unanimous New Jersey Supreme Court held that the statute contains no mental-state requirement

for actual-damages liability. Missing the ten-day takedown window incurs liability regardless of intent, good faith, or process failures.[41] The First Amendment challenge to that regime, which rests on *Sorrell*, remains pending before the Third Circuit. Liability without fault is the operative rule today. Automated and verified takedown propagation across all embedded feeds is accordingly an essential control for any vendor and for any licensee redistributing address-bearing records.

SECTION 8

Collection-side litigation: pixels and wiretap statutes

Before intent data is licensed, it is collected, ordinarily by a pixel. The most active privacy litigation in the country challenges that layer under wiretap and pen-register statutes, and it names the data vendor as well as the website operator.

8.1 CIPA § 631: interception and the timing of consent

The Ninth Circuit's published decision in *In re Facebook Internet Tracking* holds that a tracking vendor whose code causes the browser to duplicate and send the user's communications to the vendor is not a "party" to the visitor-website exchange, and therefore cannot claim the party exception to the federal Wiretap Act and CIPA § 631. The case settled for $90 million.[49] *Javier v. Assurance IQ* supplies the timing rule: consent must precede or accompany the moment recording begins, and retroactive consent through a later privacy-policy acknowledgment does not cure a pre-consent capture.[42] *Mikulsky v. Bloomingdale's* (9th Cir. 2025) lowered the pleading threshold on the distinction between contents and record information, holding that pixel payloads carrying what a person typed, clicked, searched, or viewed are "contents" of communications.[43] Outside California, *Popa v. Harriet Carter Gifts* (3d Cir., precedential) holds that Pennsylvania's two-party-consent wiretap act contains no direct-party exception and locates the interception at the visitor's browser. A tracking vendor is therefore exposed wherever its pixel loads, and the disclosure and consent language on customers' websites becomes the vendor's principal defense.[50] *Briskin v. Shopify* (9th Cir. 2025, en banc) removed the principal procedural defense: a back-end platform that extracts and commercially distributes Californians' data through customer websites is subject to California jurisdiction without any forum-specific targeting.[51]

8.2 CIPA § 638.51: the pen-register theory

Greenley v. Kochava first held that CIPA's pen-register and trap-and-trace prohibition can reach commercial tracking software that collects routing and addressing signals, including IP addresses and identifiers, in order to identify a person. The defendant was the data vendor itself.[44] Trial courts promptly divided. *Licea v. Hickory Farms* sustained a demurrer, reasoning that visiting a website is not the operation of a pen register, while *Levings v. Choice Hotels* overruled a demurrer on nearly identical allegations weeks later in the same courthouse.[45] No controlling appellate decision has resolved the question. The legislature may resolve the private theory: SB 690, as amended July 2, 2026, would confine website and application pen-register claims to the Attorney General, with retroactive effect, while leaving § 631 liability intact. The bill passed Assembly Appropriations 15 to 0 and faces an August 31, 2026 session deadline.[46]

8.3 Defense-side authority and the health-pixel cases

The leading state high-court decision for the defense is *Vita v. New England Baptist Hospital* (Mass. 2024), which held that browsing a public website is not a person-to-person "communication" under the Massachusetts wiretap act, the statute plaintiffs had most often invoked in website-tracking cases because of its statutory damages.[47] At the opposite pole, *In re Meta Pixel Healthcare Litigation*, brought against the pixel recipient rather than the website operators, survived dismissal on ECPA wiretap and privacy claims and is in class-certification briefing. Parallel suits against individual health systems have settled for amounts in the seven and eight figures.[48] A vendor ingesting pixel events from customer sites in sensitive verticals occupies the recipient's structural position.

> **Consequences for an intent pipeline.** (1) Pixels must fire after consent wherever consent is required. Pre-banner capture is the conduct charged in the *Javier* line of cases. (2) The vendor cannot delegate this obligation. Publisher-side disclosure naming the vendor, together with vendor-side contractual consent warranties, constitutes the defense. (3) Sensitive verticals such as health and finance warrant categorical treatment, as the Meta Pixel litigation demonstrates recipient-side exposure. (4) The § 638.51 theory is unresolved and should be treated as a quantifiable risk until SB 690 or an appellate ruling resolves it.[45,46] (5) The wiretap statutes regulate interception, so this exposure concentrates at the collection layer and is managed there. The licensed output contains no communications "contents," meaning no payloads, URLs, or titles. An embedded customer receiving topic scores is not receiving intercepted material, in contrast to the pixel-recipient defendants in the *Meta Pixel* litigation.[48]

SECTION 9

Sensitive categories and inference

The most consequential legal line in this area runs through inference, and it is the one place where the taxonomy-score abstraction provides no protection, because here the score itself is the regulated artifact. A scored topic is regulated not by the field it occupies but by what it can reveal.

9.1 Inference-inclusive definitions

Washington's My Health My Data Act defines "consumer health data" to include data derived or extrapolated from non-health information, expressly including inferences produced "by any means, including algorithms or machine learning." Collecting or sharing such data requires opt-in consent, and selling it requires a separate signed authorization naming the specific data, the seller, and the purchaser, valid for one year. That requirement is practically incompatible with a data-licensing model. Violations are per-se violations of Washington's Consumer Protection Act, which provides a private right of action.[56] The first MHMDA class actions were filed in February 2025 against Amazon's advertising SDK, a B2B data infrastructure defendant rather than a consumer health application. The actions were voluntarily dismissed without prejudice, so the theory remains untested and may be refiled.[57] Nevada's SB 370 mirrors the inference-inclusive definition and the written-authorization requirement for sales, with enforcement reserved to the Attorney General, and it contains a usable exclusion: shopping habits and interests are excluded if not used to identify health status.[58] Connecticut incorporated MHMDA-style consumer health data into its omnibus statute as sensitive data requiring opt-in consent.[30]

Colorado's Attorney General rules contain the most explicit US statement on browsing-derived inference. "Sensitive Data Inferences" are inferences from personal data used to indicate health, religion, sex life or sexual orientation, race, or citizenship, and the rules provide their own example: web browsing data that infers sexual orientation is sensitive data. Opt-in consent is required, and the narrow exemption (deletion within 24 hours and no transfer) is by definition unavailable to a licensing business.[27] California reaches sensitive status through its "collected and analyzed concerning a consumer's health" formulation,[19] and the Healthline judgment prohibited article-title signals revealing a diagnosis outright.[24] Maryland prohibits the sale of sensitive data, including use-based health data, sexuality, and religion, with no consent exception.[32]

9.2 Federal and EU reinforcement

The FTC's Gravy Analytics order treats sensitive characteristics derived from behavioral data as themselves the regulated product.[11] The amended Health Breach Notification Rule makes unauthorized disclosure of identifiable health data by any online service that tracks health conditions a federally reportable "breach" carrying civil penalties, an exposure that reaches embedded customers who build health-adjacent features.[59] In the EU, the Grand Chamber's *OT*

judgment holds that data liable to disclose a sensitive trait indirectly is special-category data,[82] and *Meta Platforms v. Bundeskartellamt* applies that holding to website-visit data specifically.[75]

9.3 The industry standard

The NAI's February 2026 Factor Analysis for health-related sensitive information, which analyzes the Healthline settlement, concludes that using health-suggestive content titles "to segment or profile a consumer as having a specific condition" weighs toward sensitive classification, while transient contextual use does not.[90] NAI guidance has required opt-in consent for health-related interest-based advertising for more than a decade.[91]

9.4 Sensitivity classification inside the taxonomy

The rules above are enforceable only if sensitivity is a property of the topic record itself, determined before any score ships, and the Delivr.ai standard taxonomy is built on that principle. Every topic carries a per-topic sensitivity classification field alongside its three-level category hierarchy.[103] In the August 2026 build, 198 of 59,070 active topics, or three tenths of one percent, are flagged Sensitive, concentrated in regulated-content verticals: alcohol and spirits (66), politics (58), cannabis (30), and gambling (27). The politics flag corresponds directly to statutory territory, as Colorado's inference rules and GDPR Article 9 treat political opinions as protected categories.[27,82] The alcohol, cannabis, and gambling flags implement care beyond current statutory minimums, consistent with the NAI's sensitive-segment guidance.[91]

The statutory sensitive-data categories of Section 9.1, namely health conditions, sexuality, religion, race, and immigration status, are addressed through two mechanisms operating together. The category hierarchy makes candidate topics structurally identifiable; the Health group, for example, comprises 2,265 active topics addressable as a block for state-specific suppression or gating. The per-topic sensitivity field is the enforcement point at which a statutory classification attaches to an individual topic. The figures describe the current build. The classification field exists so that the flagged set can track the statutory map of Section 9.1 as it develops. Washington's inference-inclusive health definition, Maryland's prohibition on sensitive-data sales, and Colorado's sensitive-data-inference rules each define the regulated set differently, and per-state treatment attaches to the topic record.[56,32,27]

> **Design consequence.** Among the taxonomy's 59,070 active topics, any topic that corresponds to a health condition, sexuality, religion, race, precise location, or immigration status must be treated as a separately regulated class: suppressed by default, gated on opt-in consent where a state permits sale with consent, excluded entirely for Maryland residents, and excluded or authorization-gated for Washington and Nevada residents. Licensing agreements should prohibit embedded customers from using non-sensitive topics to identify sensitive status, which is the use-based trigger in the Washington, Nevada, Connecticut, and Maryland definitions.[56,58,30,32]

The per-topic sensitivity classification in the taxonomy (Section 9.4) is the mechanism to which each of these treatments attaches.[103]

SECTION 10

Sectoral boundaries: VPPA, FCRA, COPPA

Three older federal statutes create categorical boundaries that an intent-data license must draw around video signals, eligibility uses, and children.

10.1 VPPA: video-derived signals

The Video Privacy Protection Act prohibits a video tape service provider from knowingly disclosing information identifying a person as having requested specific video materials. It provides liquidated damages of $2,500 per person and a consent regime requiring a distinct, standalone authorization.[60] Pixel litigation reached the statute. *Salazar v. NBA* (2d Cir. 2024) held that a newsletter subscriber is a protected "consumer," so that transmitting a Facebook ID together with video-watching history states a claim.[61] *Salazar v. Paramount* (6th Cir. 2025) reached the opposite conclusion on the same facts.[62] The Supreme Court granted certiorari in January 2026 to resolve the split, with argument expected in the October 2026 term.[63] Until the Court rules, the broader Second Circuit reading is the operative compliance standard: video-consumption signals tied to specific titles should be aggregated above the title level or excluded from person-level feeds.

10.2 FCRA: the eligibility boundary

Person-level interest profiles bear on "personal characteristics" and "mode of living," so FCRA status turns on use and expected use. Data used, or expected to be used, to establish eligibility for credit, insurance, or employment is a consumer report, and its regular assembler is a consumer reporting agency.[64] The FTC's Spokeo settlement ($800,000) establishes that a marketing-data broker becomes a consumer reporting agency based on how it markets the data; there, person-level profiles were marketed to human resources and recruiting customers.[65] The CFPB's December 2024 proposal to classify data brokers as consumer reporting agencies by rule was withdrawn in May 2025. The withdrawal leaves the use-based statutory boundary in place, so a contractual prohibition on all eligibility uses remains the control that keeps intent data outside the FCRA.[66] The DAA's Multi-Site Data Principles have prohibited eligibility uses of cross-site data since 2011 and supply the industry-standard clause language.[92]

10.3 COPPA: children

The 2025 COPPA amendments require separate verifiable parental consent for third-party disclosures, a provision directed at targeted advertising, together with a written, published data retention policy specifying deletion timeframes.[67] Child-directed properties will rarely hold the required opt-in consent, so the workable rule for a person-level product is exclusion: the vendor warrants that the graph excludes known child-directed sources, and the license prohibits application of the data to users under thirteen.

SECTION 11

National-security transfer restrictions: PADFAA and the DOJ rule

Since 2024, two federal regimes restrict the parties to whom licensed personal data may be transferred, and browsing-derived intent data falls expressly within both.

The Protecting Americans' Data from Foreign Adversaries Act (PADFAA) makes it unlawful for a data broker to make personally identifiable sensitive data of US individuals available to a foreign adversary country or to an entity controlled by one. "Sensitive data" expressly includes "information identifying an individual's online activities over time and across websites," and "controlled by" reaches twenty percent ownership. Violations are treated as rule violations under the FTC Act, so civil penalties are available for a first violation.[68] Enforcement has begun. In February 2026, the FTC sent warning letters to thirteen data brokers concerning products involving Armed Forces membership status, citing penalties of up to $53,088 per violation. Attribute-level segments were the conduct that drew the letters.[69]

The DOJ's Data Security Program (28 C.F.R. Part 202, effective April 8, 2025) prohibits US persons from knowingly engaging in "data brokerage," defined as the sale or licensing of data to a recipient that did not collect it directly, involving countries of concern (China, Cuba, Iran, North Korea, Russia, and Venezuela) or covered persons.[70] Hashed emails and device IDs are "covered personal identifiers," and the bulk threshold is crossed at 100,000 US persons, a level that essentially every commercial licensing arrangement will meet.[72] For transactions with any foreign person, § 202.302 mandates a contractual onward-transfer prohibition together with a duty to report suspected violations to the DOJ within fourteen days.[71]

> **Contract consequence.** Screening customers for adversary ownership and covered-person status is now a legal requirement rather than a diligence practice. Every license to a non-US customer requires the § 202.302 onward-transfer clause, and every license, domestic or foreign, should carry adversary-ownership representations with a change-of-control trigger.[70,71]

SECTION 12

EU and UK law: why licensed intent data is scoped to US persons

For EU and UK data subjects, four independent legal barriers apply cumulatively. Together they explain why a person-level intent product is scoped to US persons rather than offered as compliant in Europe.

- **Consent is required at the point of collection, regardless of hashing.** Article 5(3) of the ePrivacy Directive conditions any storage of, or access to, information on a user's device, including cookies and pixels, on prior informed consent.[73] *Planet49* holds that the rule applies whether or not the information is personal data, and that consent must be active rather than pre-selected.[74]
- **Legitimate interests cannot support behavioral profiling for advertising.** The Grand Chamber in *Meta Platforms v. Bundeskartellamt* held that collecting data on users' visits to third-party websites and applications, linking it to accounts, and using it for personalized advertising cannot rest on Article 6(1)(f), because users cannot reasonably expect such processing and their rights override the advertising interest. Nor does the processing qualify as contractual necessity, since personalization is not objectively indispensable to the service.[75,76] The UK tribunals in *Experian* left legitimate interests available for certain offline marketing data, but they prohibited repurposing consent-sourced data under legitimate interests and held that individuals who never received an Article 14 notice were processed unlawfully. Transparency at data-broker scale is the practical obstacle.[84,85]
- **The vendor must itself hold proof of consent it did not collect.** The CNIL fined Criteo forty million euros, holding that delegating consent collection to publisher partners "does not exempt the company from its obligation ... to be able to demonstrate" each data subject's consent.[77] The Belgian DPA's IAB Europe decision, which held that TC Strings are personal data, that the framework operator is a joint controller, and that legitimate interest is unavailable for real-time bidding, was confirmed in substance by the CJEU in 2024 and by the Brussels Market Court in 2025.[78,80,79] The EDPB has further concluded that "consent or pay" mechanisms on large platforms will in most cases fail the freely-given standard,[83] and the CJEU places the burden of proving valid consent on the operator even where consent is available.[75]
- **Sensitive inference and scoring rules apply with the greatest force.** Browsing data liable to reveal health, religion, politics, or sexuality is Article 9 special-category data, prohibited in principle, and mere browsing does not qualify for the "manifestly made public" exception.[82,75] *SCHUFA* holds that a vendor's automated score is itself an Article 22 automated decision when customers give it a determining role.[81]

The identifier-level analysis, comprising *Breyer* relative identifiability and *EDPS v. SRB* recipient-relative pseudonymisation, is addressed in Section 5.2.[52,53] The operational conclusion is that EU and UK data subjects are excluded from the licensed dataset, that license agreements state the exclusion expressly, and that customers are prohibited from applying the data to EU or UK residents.

SECTION 13

Downstream liability and required contract terms

The consistent principle of the modern enforcement record is that a data licensor answers for its supply chain in both directions, and that the contract is the first place regulators examine.

13.1 The liability foundation

FTC v. Accusearch (10th Cir. 2009) is the appellate foundation. A data reseller was held liable under Section 5 for the manner in which its researchers obtained telephone records and for the foreseeable injuries its sales enabled. Its intermediary status and platform-immunity arguments failed.[87] *FTC v. Sitesearch (LeapLab)* extends the principle downstream: selling consumer data to buyers with no legitimate need was itself the unfair practice, aggravated by continued sales after the seller learned of a buyer's fraud.[88] On the private side, *Katz-Lacabe v. Oracle*, which asserted intrusion, CIPA, and UCL claims over person-level profiles assembled from web behavior and sold through a data marketplace, settled for $115 million with injunctive limits on collection. The case establishes that tort exposure attaches at assembly and sale, independent of any downstream misuse.[86]

13.2 The statutory contract floor

California requires a written agreement for every sale, share, or disclosure of personal information, containing five elements: purpose limitation, recipient compliance with the CCPA at the same level of protection, oversight rights, notice if the recipient can no longer comply, and rights to stop and remediate unauthorized use.[20] The CPPA's Honda order establishes that these clauses are independently enforceable. The penalty issued in part for failure to produce conforming contracts, without any showing of downstream misuse.[25] Whether an embedded customer is a "third party," in which case the transfer is a sale and opt-outs are required, or a "service provider," in which case processing is contract-restricted, turns entirely on these terms. That is the lesson of Sephora.[22]

13.3 Requirements added by the FTC orders

- Supplier assessments within 30 days of any data-sharing agreement, verifying consumer consent up the chain (X-Mode).[6]
- Written supplier certifications of authority to provide the data; sampling-based review was expressly identified as inadequate (Mobilewalla).[10]
- Downstream use restrictions on recipients, including prohibitions on sensitive-location association and on identification of individuals (X-Mode), and restrictions on resale (Gravy).[6,12]
- Deletion that propagates, through instructions to customers to delete data and derived work product (Mobilewalla, Gravy).[10,12]

- Incident reports to the FTC when a third party shares data in violation of its contract (Kochava).[4]

13.4 The industry frameworks that operationalize these duties

The IAB's Multi-State Privacy Agreement, the prevailing contractual architecture for person-level data in US programmatic advertising, treats disclosure for "Third-Party Segment Creation" as a CCPA sale, prohibits passing an opted-out consumer's data downstream, resolves conflicting signals in favor of the more restrictive processing, imposes accountability on any participant that re-sells, and incorporates the California contract clauses.[95] The Global Privacy Platform is the signal layer that carries opt-out and consent state through the chain, and MSPA signatories are contractually obligated to send, receive, and honor it.[96] The NAI's 2025 Framework binds members to transparency, consumer choice, data governance, sensitive-data safeguards, and annual accountability reviews.[89] The DAA principles have governed cross-site and cross-device data since 2009, with published enforcement decisions and FTC referral as the backstop.[93,94] At the identifier layer, UID2, the token generated from SHA-256 hashed emails, carries its own contractual controls: sharing is permitted only among parties bound by the Participation Policy, and a global opt-out portal propagates to all participants.[97,98] LiveRamp's RampID documentation reflects the parallel market posture of deterministic matching, pseudonymization at the identifier layer, and a non-discoverable graph.[99]

13.5 The clause checklist

CLAUSE	SOURCE OF THE DUTY
Purpose limitation to enumerated embedded uses; no re-identification of individuals beyond the licensed resolution scope	Cal. Civ. Code § 1798.100(d)[20]; Avast (re-identification-enabling terms treated as an aggravating factor)[13]
No eligibility uses: credit, insurance, employment, tenancy, or health-care treatment	FCRA use-based boundary[64]; Spokeo order[65]; DAA Multi-Site § II[92]
No use of any topic to identify sensitive status; sensitive-category segments excluded or consent-gated by state	WA/NV/CT/MD health-data laws[56,58,30,32]; CO Rule 6.10[27]; FTC orders[11]
Opt-out and deletion propagation: GPC and universal opt-out honoring, DROP-driven deletion within 45 days, Daniel's Law takedown flow-down	Sephora, Honda[22,25]; Delete Act[34]; Atlas (liability without fault)[41]
Rights to stop and remediate, audit rights, termination on misuse; customer vetting for	§ 1798.100(d)[20]; LeapLab[88]

CLAUSE	SOURCE OF THE DUTY
legitimate need	
Onward-transfer prohibition naming countries of concern; adversary-ownership representations; a 14-day DOJ reporting process	28 C.F.R. §§ 202.301–.302[70,71]; PADFAA[68]
No application to users under thirteen or to child-directed services; no title-level video disclosures absent VPPA-compliant consent; no EU or UK data subjects	COPPA 2025[67]; VPPA and the Salazar litigation[60,61]; Section 12 authorities
Deletion of licensed data and derived work product on instruction; notice upon inability to comply	Mobilewalla and Gravy orders[10,12]; § 1798.100(d)[20]

In Delivr.ai's contract architecture, these clauses attach through the data-rights tier system. Tier 2 (Embedded Use) and Tier 3 (Distribution) grants carry permitted data product, approved end-customer category, and volume-limit terms written into the order form, with the use restrictions above flowing down to the customer's own downstream users. This is the structure that the MSPA's resale accountability rules and the FTC's order templates each contemplate.[95,6]

SECTION 14

Litigation defenses and open questions

The record is not one-directional. Several doctrines materially limit exposure, and several questions are presently before the courts and the legislature.

14.1 Defenses

- **First Amendment.** *Sorrell* holds that the sale and dissemination of person-identified information for marketing is protected expression, and that content-based and speaker-based restrictions receive heightened scrutiny.[102] It is the basis of the pending Daniel's Law challenge.[41]
- **Article III standing.** *Spokeo*, itself a case concerning a data broker's person-level profiles, requires concrete harm beyond a bare statutory violation.[101] *TransUnion* holds that records merely maintained, without dissemination, cause no concrete defamation-type harm.[100] Federal statutory-damages classes premised on data that was held but not shared fail at the threshold.
- **Statutory construction.** *Vita* removes the Massachusetts wiretap act from website-tracking cases.[47] *Solomon* and the Sixth Circuit's *Salazar* decision narrow the VPPA's "personally identifiable information" and "consumer" terms in at least three circuits.[55,62] *Licea* demonstrates the pen-register theory failing in reasoned trial-court decisions.[45]
- **Recipient-relative pseudonymisation (EU).** *EDPS v. SRB* confirms that strongly pseudonymised data can fall outside the GDPR for a recipient lacking the means of re-identification.[53] The holding is relevant to narrowly aggregated or non-resolvable deliverables, though not to resolution products.

14.2 Open questions

QUESTION	VEHICLE	POSTURE AS OF AUGUST 2026
Does the VPPA protect all customers of a video provider or only audiovisual subscribers?	*Salazar v. Paramount*, No. 25-459 (U.S.)	Certiorari granted January 26, 2026; argument expected in the October 2026 term[63]
Is Daniel's Law's liability without fault constitutional under the First Amendment?	Third Circuit, No. 25-1555	The New Jersey Supreme Court has answered the state-law question (no mental-state requirement); the constitutional question remains pending[41]

QUESTION	VEHICLE	POSTURE AS OF AUGUST 2026
Will private pen-register claims over website tracking survive?	California SB 690	Passed Assembly Appropriations 15 to 0; must clear both chambers by August 31, 2026; would confine § 638.51 website claims to the Attorney General, with retroactive effect[46]
Will data brokers be classified as consumer reporting agencies by rule?	CFPB FCRA rulemaking	Withdrawn May 15, 2025; the Bureau has stated that its FCRA interpretation is under revision, so the question may return[66]
How far does the MHMDA private right of action reach B2B data infrastructure?	Refiled actions in the pattern of the Amazon SDK cases	The first actions were voluntarily dismissed without prejudice in June 2025; the theory is untested[57]

SECTION 15

Compliance checklist for embedded data customers

The obligations an embedded data customer assumes with a person-level intent license. Each row names the statute, order, or case that imposes it.

#	OBLIGATION	AUTHORITY
1	Disclose the data relationship in the privacy notice; where data is re-disclosed for advertising, treat the disclosure as a sale or share with an operating opt-out and GPC honoring	CCPA §§ 1798.120, 1798.140; Sephora; Honda and Todd Snyder[19,22,25]
2	Execute and retain the required contract clauses; regulators have imposed penalties for their absence alone	§ 1798.100(d); Honda[20,25]
3	Determine whether the customer independently qualifies as a data broker (no direct relationship with the scored individuals, combined with sale or licensing); if so, register in California, Vermont, Texas, and Oregon, and implement DROP deletion	Delete Act; CalPrivacy advisory (no reliance on a parent's registration); Vermont; Texas ch. 509; Oregon[34,35,37,38,40]
4	Do not use intent data for eligibility decisions concerning credit, insurance, employment, tenancy, or health care	FCRA; Spokeo; DAA § II[64,65,92]
5	Do not use any topic to identify a health condition or other sensitive status; honor the per-topic sensitivity classifications delivered with the taxonomy and the license's sensitive-category exclusions; assume the Washington, Nevada, Connecticut, and Maryland rules apply at the person level	MHMDA; NV SB 370; CT PA 23-56; MODPA; CO Rule 6.10[56,58,30,32,27]
6	Propagate deletions and takedowns within the contractual service levels; Delete Act cycles run 45 days, and Daniel's Law allows 10 days with liability regardless of fault	Delete Act; Atlas[34,41]

#	OBLIGATION	AUTHORITY
7	Where the customer's own product fires tracking on its pages, sequence consent before capture and name data partners in disclosures	Javier; Popa; Facebook Tracking[42,50,49]
8	Screen downstream recipients for foreign-adversary ownership; include onward-transfer clauses; report suspected violations	PADFAA; 28 C.F.R. § 202.302[68,71]
9	Exclude the data from EU and UK use cases and from audiences under thirteen	Section 12 authorities; COPPA 2025[67]
10	Describe the data accurately: pseudonymous personal information, deterministically matched, delivered as taxonomy topic scores with no underlying URLs, titles, or events; never described as anonymous, and never described as browsing data	FTC hashing guidance; Avast; Mobilewalla[17,13,9]
11	Prepare for access requests that reach the scores themselves and, in Oregon, for naming specific recipients	Cal. AG Op. 20-303; OCPA[21,33]
12	Aggregate video-consumption signals above the title level absent VPPA-compliant consent, pending the Supreme Court's decision	VPPA; the Salazar litigation[60,61,63]

SECTION 16

References

Sources 1 through 102 were verified by direct retrieval on August 24, 2026. Citations to press releases of the FTC, state attorneys general, and the CPPA refer to the enforcing agency's own announcement of the underlying complaint, order, or judgment. Source 103 is an internal Delivr.ai data source, verified by direct inspection on August 27, 2026.

1. FTC v. Kochava, Inc., No. 2:22-cv-00377-BLW (D. Idaho, filed Aug. 29, 2022), FTC press release and complaint. ftc.gov
2. FTC v. Kochava, Inc., No. 2:22-cv-00377-BLW, Dkt. 71, Memorandum Decision and Order (D. Idaho Feb. 3, 2024) (Winmill, J.). ftc.gov (opinion PDF)
3. FTC v. Kochava, Inc., No. 2:22-cv-00377-BLW, order denying motion to dismiss Second Amended Complaint (D. Idaho Feb. 3, 2025). govinfo.gov
4. FTC v. Kochava, Inc., stipulated final order (announced May 4, 2026). ftc.gov
5. In the Matter of X-Mode Social, Inc. and Outlogic, LLC, FTC File No. 2123038 (proposed order Jan. 9, 2024; finalized Apr. 2024). ftc.gov
6. X-Mode/Outlogic, FTC analysis of proposed consent order, 89 Fed. Reg. (Jan. 18, 2024). govinfo.gov
7. In the Matter of InMarket Media, LLC, FTC File No. 2023088 (final order May 1, 2024). ftc.gov
8. InMarket, FTC analysis of proposed consent order, 89 Fed. Reg. 4301 (Jan. 23, 2024). govinfo.gov
9. In the Matter of Mobilewalla, Inc., FTC File No. 202-3196 (proposed order Dec. 3, 2024; finalized 2025). ftc.gov
10. Mobilewalla, FTC analysis of proposed consent order, 89 Fed. Reg. 96996 (Dec. 6, 2024). govinfo.gov
11. In the Matter of Gravy Analytics, Inc. and Venntel, Inc., FTC File No. 212-3035 (proposed order Dec. 3, 2024; finalized Jan. 2025). ftc.gov
12. Gravy Analytics/Venntel, FTC analysis of proposed consent order, 89 Fed. Reg. (Dec. 6, 2024). govinfo.gov
13. In the Matter of Avast Limited, FTC File No. 2023033 ($16.5M; proposed order Feb. 22, 2024; finalized June 2024). ftc.gov
14. In the Matter of BetterHelp, Inc., FTC Docket No. C-4796 (final order July 14, 2023; $7.8M). ftc.gov
15. United States v. GoodRx Holdings, Inc., FTC File No. 2023090 (N.D. Cal., Feb. 1, 2023; $1.5M HBNR penalty). ftc.gov
16. In the Matter of General Motors LLC and OnStar LLC, FTC File No. 2423052 (proposed Jan. 16, 2025; finalized Jan. 2026). ftc.gov
17. FTC Office of Technology, "No, hashing still doesn't make your data anonymous" (July 24, 2024). ftc.gov

18. Ed Felten (FTC Chief Technologist), "Does Hashing Make Data 'Anonymous'?" (Apr. 22, 2012). ftc.gov
19. Cal. Civ. Code § 1798.140 (definitions: sell (ad), share (ah), personal information and inferences (v)(1), sensitive personal information (ae), unique identifier (aj), profiling (z)); § 1798.121 (right to limit). leginfo.legislature.ca.gov
20. Cal. Civ. Code § 1798.100(d) (mandatory contract terms). leginfo.legislature.ca.gov
21. Cal. Op. Att'y Gen. No. 20-303 (Mar. 10, 2022) (internally generated inferences disclosable). oag.ca.gov
22. People v. Sephora USA, CCPA settlement, $1.2M (Aug. 24, 2022). oag.ca.gov
23. People v. DoorDash, CCPA/CalOPPA stipulated judgment, $375,000 (Feb. 21, 2024). oag.ca.gov
24. People v. Healthline Media, CCPA settlement, $1.55M (July 1, 2025). oag.ca.gov
25. CPPA Stipulated Final Orders: In re American Honda Motor Co. ($632,500, Mar. 12, 2025); In re Todd Snyder, Inc. ($345,178, May 6, 2025). cppa.ca.gov
26. Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 et seq.; universal opt-out mandatory July 1, 2024. coag.gov
27. Colorado Privacy Act Rules, 4 CCR 904-3, Rules 2.02 and 6.10 (sensitive data inferences). coag.gov (PDF)
28. Virginia Consumer Data Protection Act, Va. Code § 59.1-575 et seq. law.lis.virginia.gov
29. Connecticut Data Privacy Act, Conn. Pub. Act No. 22-15, Conn. Gen. Stat. § 42-515 et seq. portal.ct.gov
30. Conn. Pub. Act No. 23-56 (consumer health data amendments to the CTDPA). cga.ct.gov (PDF)
31. Texas Data Privacy and Security Act, Tex. Bus. & Com. Code ch. 541 (H.B. 4, 2023); State of Texas v. Allstate Corp. et al., No. 25-01-00561 (457th Dist. Ct., Montgomery Cnty., filed Jan. 13, 2025). capitol.texas.gov
32. Maryland Online Data Privacy Act, Md. Code Ann., Com. Law § 14-4601 et seq. (2024 Md. Laws ch. 455, S.B. 541). mgaleg.maryland.gov (PDF)
33. Or. Rev. Stat. §§ 646A.570–.589; Oregon DOJ, Six-Month Enforcement Report on the OCPA (2025). doj.state.or.us (PDF)
34. California Delete Act, Cal. Civ. Code §§ 1798.99.80–.89 (SB 362, 2023). leginfo.legislature.ca.gov
35. CalPrivacy (CPPA) Enforcement Advisory on Data Broker Registration (Dec. 17, 2025). cppa.ca.gov
36. CPPA Stipulated Final Order, In re Accurate Append, Inc. ($55,400, July 29, 2025). cppa.ca.gov
37. Vermont data broker law, 9 V.S.A. §§ 2430, 2446–2447 (Act 171 of 2018). statute text (PDF)
38. Texas data broker law, Tex. Bus. & Com. Code ch. 509 (SB 2105, 2023). texas.public.law
39. Office of the Texas Attorney General, notification of more than 100 unregistered data brokers (June 18, 2024) (press release, as republished). press release
40. Oregon data broker registration law, ORS 646A.593 (HB 2052, 2023). oregon.public.law

41. Atlas Data Privacy Corp. v. We Inform, LLC, No. A-8-25 (091145) (N.J. Aug. 12, 2026) (certified question; no mental-state requirement); constitutionality pending, 3d Cir. No. 25-1555. njcourts.gov (opinion PDF)
42. Javier v. Assurance IQ, LLC, No. 21-16351, 2022 WL 1744107 (9th Cir. May 31, 2022) (unpublished). ca9.uscourts.gov (PDF)
43. Mikulsky v. Bloomingdale's, LLC, Nos. 24-3564, 24-3837 (9th Cir. June 20, 2025) (unpublished). ca9.uscourts.gov (PDF)
44. Greenley v. Kochava, Inc., 684 F. Supp. 3d 1024 (S.D. Cal. 2023). opinion (PDF)
45. Licea v. Hickory Farms LLC, No. 23STCV26148 (Cal. Super. Ct. L.A. Cnty. Mar. 13, 2024); Levings v. Choice Hotels Int'l, No. 23STCV28359 (Cal. Super. Ct. L.A. Cnty. Apr. 3, 2024) (trial-court split; unpublished orders, as reported with excerpts). case report
46. California S.B. 690, 2025–2026 Reg. Sess. (as amended July 2, 2026). leginfo.legislature.ca.gov
47. Vita v. New England Baptist Hospital, 494 Mass. 824 (Mass. Oct. 24, 2024). opinion
48. In re Meta Pixel Healthcare Litigation, No. 3:22-cv-03580-WHO (N.D. Cal.) (consolidated; class certification briefing). case docket summary
49. In re Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589 (9th Cir. 2020), cert. denied, 141 S. Ct. 1684 (2021). opinion
50. Popa v. Harriet Carter Gifts, Inc., 45 F.4th 687 (3d Cir. 2022). opinion
51. Briskin v. Shopify, Inc., 135 F.4th 739 (9th Cir. 2025) (en banc). case report
52. Breyer v. Bundesrepublik Deutschland, Case C-582/14, ECLI:EU:C:2016:779 (CJEU Oct. 19, 2016). curia.europa.eu (PDF)
53. EDPS v. SRB, Case C-413/23 P (CJEU Sept. 4, 2025). curia.europa.eu (PDF)
54. EDPB, Guidelines 01/2025 on Pseudonymisation (adopted for consultation Jan. 16, 2025). edpb.europa.eu
55. Solomon v. Flipps Media, Inc., 136 F.4th 41 (2d Cir. 2025). opinion (PDF)
56. Washington My Health My Data Act, RCW 19.373 (2023 c 191). app.leg.wa.gov
57. In re Amazon Ads SDK Litigation, No. 2:25-cv-00252-BJR (W.D. Wash.) (consolidating Maxwell v. Amazon; voluntarily dismissed June 2025). courtlistener.com
58. Nevada SB 370 (2023), NRS ch. 603A (consumer health data). leg.state.nv.us (PDF)
59. FTC Health Breach Notification Rule, 16 C.F.R. Part 318 (final rule 89 FR 47028; effective July 29, 2024). ecfr.gov
60. Video Privacy Protection Act, 18 U.S.C. § 2710. law.cornell.edu
61. Salazar v. National Basketball Association, 118 F.4th 533 (2d Cir. 2024). opinion
62. Salazar v. Paramount Global, 133 F.4th 642 (6th Cir. 2025). opinion (PDF)
63. Salazar v. Paramount Global, No. 25-459 (U.S., cert. granted Jan. 26, 2026), question presented. supremecourt.gov (PDF)

64. Fair Credit Reporting Act, 15 U.S.C. § 1681a(d), (f). law.cornell.edu

65. United States v. Spokeo, Inc., No. 2:12-cv-05001 (C.D. Cal. 2012); FTC File No. 102-3163 ($800,000). ftc.gov

66. CFPB, Protecting Americans From Harmful Data Broker Practices (Regulation V), NPRM 89 FR 101402 (Dec. 13, 2024); withdrawal 90 FR 20568 (May 15, 2025). govinfo.gov

67. FTC COPPA Rule amendments, 90 FR 16918 (Apr. 22, 2025); 16 C.F.R. §§ 312.5(a)(2), 312.10. govinfo.gov

68. Protecting Americans' Data from Foreign Adversaries Act of 2024, Pub. L. No. 118-50, div. I, 15 U.S.C. § 9901. uscode.house.gov

69. FTC, PADFAA warning letters to 13 data brokers (Feb. 2026). ftc.gov

70. DOJ, Preventing Access to U.S. Sensitive Personal Data by Countries of Concern (final rule), 90 FR 1636 (Jan. 8, 2025); 28 C.F.R. Part 202. federalregister.gov

71. 28 C.F.R. § 202.302 (onward-transfer contract requirement; 14-day DOJ reporting). law.cornell.edu

72. 28 C.F.R. § 202.205 (bulk thresholds; covered personal identifiers >100,000 U.S. persons). law.cornell.edu

73. ePrivacy Directive 2002/58/EC, Art. 5(3), as amended by Directive 2009/136/EC (consolidated text). eur-lex.europa.eu

74. Planet49 GmbH, Case C-673/17 (CJEU Oct. 1, 2019). curia.europa.eu (PDF)

75. Meta Platforms Inc. v. Bundeskartellamt, Case C-252/21, ECLI:EU:C:2023:537 (CJEU Grand Chamber, July 4, 2023). eur-lex.europa.eu

76. Meta Platforms v. Bundeskartellamt, CJEU Press Release No. 113/23 (July 4, 2023). curia.europa.eu (PDF)

77. CNIL Restricted Committee, Délibération SAN-2023-009 (June 15, 2023), CRITEO, €40M. decision (PDF)

78. Belgian DPA (APD/GBA) Litigation Chamber, Decision 21/2022 (Feb. 2, 2022), IAB Europe TCF, €250,000. dataprotectionauthority.be

79. Brussels Market Court, judgment of May 14, 2025 (IAB Europe v. Belgian DPA). dataprotectionauthority.be

80. IAB Europe v. Gegevensbeschermingsautoriteit, Case C-604/22, ECLI:EU:C:2024:214 (CJEU Mar. 7, 2024). curia.europa.eu (PDF)

81. SCHUFA Holding (Scoring), Case C-634/21 (CJEU Dec. 7, 2023). curia.europa.eu (PDF)

82. OT v. Vyriausioji tarnybinės etikos komisija, Case C-184/20, EU:C:2022:601 (CJEU Grand Chamber, Aug. 1, 2022). eur-lex.europa.eu

83. EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models (Apr. 17, 2024). edpb.europa.eu

84. Experian Ltd v. Information Commissioner, [2023] UKFTT 00132 (GRC) (Feb. 20, 2023). decision (PDF)
85. Information Commissioner v. Experian Ltd, [2024] UKUT 105 (AAC). caselaw.nationalarchives.gov.uk
86. Katz-Lacabe v. Oracle America, Inc., No. 3:22-cv-04792-RS (N.D. Cal.), $115M class settlement (final approval Nov. 15, 2024). complaint (PDF)
87. FTC v. Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009). opinion
88. FTC v. Sitesearch Corp. (d/b/a LeapLab), No. CV-14-02750-PHX-NVW (D. Ariz.; stipulated orders Feb. 2016). case summary and filings
89. NAI, Principles & Self-Regulatory Framework (Mar. 2025). thenai.org (PDF)
90. NAI, Factor Analysis for Health-Related Sensitive Personal Information (Feb. 24, 2026). thenai.org (PDF)
91. NAI, Requirements and Best Practices for Health-Related Targeting. thenai.org
92. DAA, Self-Regulatory Principles for Multi-Site Data, §§ II–III (Nov. 2011). digitaladvertisingalliance.org (PDF)
93. DAA, Self-Regulatory Principles suite (2009–present). digitaladvertisingalliance.org
94. BBB National Programs, Digital Advertising Accountability Program, Formal Review of Compare.com (June 15, 2020). decision (PDF)
95. IAB Privacy, Inc., Fifth Amended and Restated Multi-State Privacy Agreement (Mar. 5, 2026). iabprivacy.com (PDF)
96. IAB Tech Lab, Global Privacy Platform specification. iabtechlab.com
97. Unified ID 2.0 documentation, "UID2 sharing" (Participation Policy requirement). unifiedid.com
98. Unified ID 2.0 documentation, "User opt-out" (Transparency and Control Portal). unifiedid.com
99. LiveRamp Connect documentation, "RampID Methodology." docs.liveramp.com
100. TransUnion LLC v. Ramirez, 594 U.S. 413 (2021). law.cornell.edu
101. Spokeo, Inc. v. Robins, 578 U.S. 330 (2016). law.cornell.edu
102. Sorrell v. IMS Health Inc., 564 U.S. 552 (2011). law.cornell.edu (syllabus)
103. Delivr.ai Standard Intent Taxonomy, August 2026 build (internal data source): 59,070 active topics, each carrying a three-level category hierarchy and a per-topic sensitivity classification field; 198 topics flagged Sensitive (alcohol & spirits 66, politics 58, cannabis 30, gambling 27, other 17); Health category group 2,265 topics. Figures from direct inspection of the taxonomy build, August 27, 2026. Available to customers under NDA on request.