Cooley

The Law of Neural Data Licensing: The State Law Landscape and the De-Identification Question

September 28, 2026

Over the past few years, one of the more visible trends among neurotech companies has been the emergence of neural data licensing as a business model. Companies collect neural data – sometimes from consumer wearables, sometimes from participants in clinical or research studies – and then license that data to third parties, such as developers of "brain foundation models" and other neuroscience companies. What began as an incidental use of research datasets has, in some quarters, become a revenue thesis: "Brain-data-as-a-service" providers now standardize and license neural datasets for others to train large-scale "mental models." That commercial arc has the potential to intersect with efforts by states to give consumers more control over their personal data.

Five states have laws that make it unlawful or practically impossible to license neural data because they either almost prohibit it (Connecticut, Delaware and Vermont), or they require the consent of the individual whose neural data is to be sold (Colorado and Montana). Since in many cases, companies that hold neural data do not know what states the individuals reside in, licensing out neural data can be prohibitive.

In addition to state laws that prohibit or require consent for the licensing out of neural data, there are additional states that require companies that license out neural data to register as data brokers, which carry a host of operational and legal burdens. Six states run stand-alone data broker registration regimes: California, Oregon, Texas, Vermont, Connecticut and New Jersey. A seventh state, Nevada, regulates a narrower set of data brokers without requiring registration with the state, but affording individuals an ability to opt out of their data being sold or licensed.

Each of the states that regulate the licensing of neural data has different definitions of neural data and different scopes of applicability. Each of the registration laws has its own definition of who is a "data broker," what kind of data triggers the registration requirement and what thresholds and exemptions apply.

Four structural models of data broker laws are now in play.

Model 1: California

California's long-standing data broker law defines "data broker" as a business that knowingly collects and sells to third parties "the personal information of a consumer with whom the business does not have a direct relationship." The law applies to a broad definition of "personal information" – any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

The law classifies neural data as a category of "sensitive personal information," which is a subset of personal information under the law. The definitional path is short: Neural data that is identifiable to an individual is sensitive personal information; sensitive personal information is personal information; and personal information triggers the data broker regime. As a result, selling identifiable neural data about individuals with whom the business has no direct relationship falls within California's data broker regime, even when the neural data is transferred without accompanying identifiers – unless the neural data has been de-identified to the California Consumer Privacy Act's (CCPA) exacting standard, in which case it is excluded from "personal information" and out of scope of the law. Whether neural data can meet that de-identification standard is a threshold question discussed later in this article.

The operational obligations are substantial. For example, registered data brokers must:

- Post a privacy policy that contains certain disclosures and offers certain consumer rights.

- Pay a $6,000 annual registration fee (increased to $9,500 in 2027), plus payment processing fees, during the January 1 – 31 registration period.
- Create and maintain a Delete Request and Opt-Out Platform (DROP) account, download the CPPA's consumer deletion list at least every 45 calendar days, and delete the consumer's personal information (including deletion by service providers and contractors) upon match.
- Process every deletion request received during the previous access session and report a response code back to the DROP ("Record deleted," "Record opted out of sale," "Record exempted" or "Record not found") at each subsequent access.
- Make enhanced disclosures during registration, including whether the data broker has shared for purposes of cross context behavioral advertising, or sold data to specific recipient categories, in the past year and identifying the most common types of personal information collected.

The CCPA regulations also refine the "direct relationship" question in a way that matters for neurotech companies: For the data broker law **not** to apply, a consumer must have intentionally interacted with the business to access, purchase, use, request or obtain information about the business's products or services. Collecting data "directly from the consumer" does not, by itself, create a direct relationship if the consumer's intent to interact with the business is missing – a distinction that matters for research-participant and clinical-trial datasets that later flow into licensing arrangements. The California law affords data brokers some exceptions from consumers' deletion rights.

Model 2: Connecticut, Oregon and Vermont – Enumerated 'brokered personal data'

Three states – Connecticut, Oregon and Vermont – apply to a specifically enumerated list of "brokered" personal data information. The list varies in the details, but the shape is consistent: name; address; date of birth; place of birth; mother's maiden name; unique biometric data used to identify or authenticate the consumer; the name or address of a member of the consumer's immediate family or household; Social Security or other government-issued identification number; and a catch-all for "other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty" (Connecticut and Vermont), or "can reasonably be associated with the individual" (Oregon).

Neural data is not one of the enumerated categories in any of these three statutes. It is pulled into these regimes only in three specific circumstances:

- **Bundling with enumerated identifiers.** The license package also contains one or more of the enumerated identifiers (name, address, date of birth, Social Security number or the like) alongside the neural data.
- **Biometric identification or authentication.** The neural data is itself being used by the licensor or licensee to identify or authenticate the consumer, bringing it under the "unique biometric data" prong. This prong requires an actual identification or authentication use – not merely that the data could theoretically be used that way. Neurotech companies whose license value proposition is training AI, not identifying users, are typically outside this prong. However, the Oregon law leaves a possibility that biometric information need not be used to identify an individual in order to be covered by the Oregon data broker law.
- **The identifiability catch-all.** The neural data itself, alone or in combination with other data, would allow a reasonable person to identify the consumer with reasonable certainty (Connecticut/Vermont) or can reasonably be associated with the individual (Oregon). This is where the de-identification question lands.

The registration and mechanics vary across these three states. Oregon has required registration since January 1, 2024, with a $600 annual fee paid through the Oregon Division of Financial Regulation, an opt-out disclosure requirement and no state-run deletion mechanism. Vermont has required registration since January 1, 2019 – the first-in-the-nation data broker registration law – with a $100 annual filing to the secretary of state, security-program requirements and enforcement by the Vermont attorney general. Connecticut's new regime turns on January 1, 2027; the Commissioner must stand up the state's accessible deletion mechanism by July 1, 2028, and data brokers must begin honoring deletion requests received through it by October 1, 2028; annual public transparency statements begin July 1, 2029; and the first triennial independent audits must be completed by July 1, 2031.

In Connecticut and Vermont, separate laws, if they apply to a business, prohibit the sale of neural data absent the

consent of the individuals whose neural data is to be sold. If these laws apply to a business, and they do not have the requisite consent, they cannot license neural data, and therefore the data broker registration requirement becomes moot.

Model 3: The Texas outlier – A revenue-based test

Texas takes a structurally different approach. The Texas Data Broker Act defines "data broker" as a business entity that collects, processes or transfers personal data that the business entity did not collect directly from the individual to whom the data is linked or linkable. "Personal data" for these purposes is broad and includes information linked or reasonably linkable to an identified or identifiable individual.

But Texas layers a materiality test on top of the definition. The law applies only to a business that, in a 12-month period, derives more than 50% of its revenue directly from processing or transferring personal data not collected by the data broker directly from the individuals to whom the data pertains, or any amount of revenue directly from processing or transferring the personal data of more than 50,000 individuals. Registration is a $300 filing with the Texas secretary of state. Obligations include a website notice identifying the business as a data broker, a comprehensive information security program, and civil penalties of $100 per day, capped at $10,000 per year, plus unpaid registration fees for noncompliance.

The practical implication for neurotech companies: Texas structurally protects businesses whose principal revenue is from selling another product or service, even where they engage in some downstream neural data licensing. The Texas law applies to pure-play "data-as-a-service" licensors of identifiable neural data and businesses with sizeable licensed-out populations. Texas also expressly exempts genuinely de-identified data, on essentially the CCPA-style standard: reasonable technical measures to prevent re-identification, a public commitment not to re-identify and contractual downstream controls.

Model 4: New Jersey – Highest fees in the nation and a novel 'data collector' concept

New Jersey enacted its data broker law on June 30, 2026 – introduced, passed and signed within a 48-hour window – making it the sixth state with a stand-alone data broker registration regime and, by a wide margin, the most expensive and structurally most disruptive. Unlike every other state's data broker law, the New Jersey law regulates not only "data brokers" (the traditional definition) but a novel second category called "data collectors" – first-party businesses that sell or license their own customers' personal data to data brokers. The law also imposes a categorical prohibition on the sale or licensing of "sensitive data," which took effect immediately upon enactment. But this ban does not apply to neural data, unless it is swept into the prohibition where the neural data reveals mental or physical health condition, treatment or diagnosis of an individual, or where the neural data is processed for the purpose of biometrically identifying an individual. Enforcement rests with the New Jersey attorney general through the Division of Consumer Affairs, and the law contains exceptions that apply in certain circumstances.

Within days of enactment, however, the law drew immediate backlash over its unusually high fees, severe penalties and novel coverage of "data collectors." A senior official from the administration of Gov. Mikie Sherrill confirmed to the press that the state would not enforce the law until the legislature fixes "certain defects that have come to light," and, on July 10, 2026, the Division of Consumer Affairs issued a public alert stating that covered data brokers and data collectors will not be required to register or pay any registration fees until the registry launches in spring 2027. The sensitive data sale prohibition, by contrast, has not been paused and remains enforceable now, although that ban does not expressly apply to neural data.

The "data collector" category is the structural novelty. A "data broker" is defined much as in other states – an entity that knowingly collects or purchases the personal data of consumers with whom it has no direct relationship, and sells or licenses that data to third parties. A "data collector," by contrast, has no analog in any other state's data broker statute. A data collector is a business that has a direct relationship with the consumer (the individual is or was a customer, subscriber, research subject or similar counterparty) but sells or licenses those consumers' personal data to a data broker downstream. A consumer neurotech company (for example, a wearable manufacturer that sells or licenses its own users' neural data downstream to a data broker) is a data collector under New Jersey law, and it is subject to the same registration, fee, disclosure and sensitive data sale prohibition obligations as a traditional broker.

Registration fees are graduated based on the number of New Jersey residents whose personal data is sold or licensed: $5,000 for 100,000 residents or fewer; $10,000 for 100,001 to 499,999; $100,000 for 500,000 to 999,999; $500,000 for 1,000,000 to 1,499,999; $750,000 for 1,500,000 to 2,499,999; $1,000,000 for 2,500,000 to 4,499,999; and $1,500,000 for 4.5 million or more. These are the highest data broker registration fees enacted by any state – the top tier alone is 250 times California's $9,500 2027 fee. Failure to register or pay the fee is a civil penalty of $2,500 per day; failure to submit or update required disclosures is the same. The law separately bans the sale, offer for sale or licensing of "sensitive data," carrying a civil penalty of $50,000 per record.

The shared thread: The 'direct relationship' carve-out

Most of the state data broker regimes turn on the presence or absence of a direct relationship between the business and the individual whose data is at issue. Under California, Connecticut, Oregon, Texas and Vermont, if the neurotech company sits at the source – the individual is (or was) a customer, a research subject under contract, an investor, a donor or in a similar direct relationship – the business is not a data broker when it licenses out that data. New Jersey is the outlier because of its additional category of "data collector." As discussed above, New Jersey's "data collector" category closes the direct relationship exception for any first-party neurotech company that sells or licenses personal data to a downstream data broker. Whether the New Jersey law applies to a business that has a relationship with the individuals whose data is being licensed depends on what the licensee does with the data downstream. Therefore, diligencing (and contractually constraining) the recipient's own resale and relicensing conduct is central to the New Jersey analysis.

State restrictions on sale of neural data

In addition to state data broker registration requirements and consumer opt-out rights, two states (Colorado and Montana) have separate laws that, if they apply, prohibit the sale of neural data of their state residents absent consent from the individuals whose neural data is to be sold, or impose such restrictions on the sale of neural data that it is impractical even with consent (Vermont, Delaware and Connecticut).

Colorado and Connecticut

The Colorado and Connecticut laws apply to essentially any business that sells or licenses out neural data.

Vermont

The Vermont law only applies to businesses that conduct business in Vermont or produce products or services that are targeted to residents of Vermont, **and** control or process the personal data of 35,000 or more Vermont residents, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; control or process the sensitive data (including neural data) of 3,000 or more Vermont residents, excluding personal data controlled or processed solely for the purposes of completing a payment transaction; or offer for sale in trade or commerce the personal data of 3,000 or more Vermont residents

Many businesses that wish to license neural data will likely not be covered by the Vermont law because they do not have a consumer-facing business and do not have a business presence in Vermont or do business with Vermont entities.

Delaware

The Delaware law applies to businesses that conduct business in Delaware or produce products or services that are targeted to residents of Delaware, **and** control or process the personal data of 10,000 or more Delaware residents, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; control or process the personal data of 5000 or more Delaware residents, and derive more than 20% of their gross revenue from the sale of personal information; or acquired personal data from another entity that is covered by the law

Some businesses that wish to license neural data will not be covered by the Delaware law because they do not have a consumer-facing business and do not have a business presence in Delaware or do business with Delaware entities.

Montana

The Montana law applies to entities that either offer consumer genetic testing products or services directly to a consumer or that collect, use or analyze genetic data. Many businesses that wish to license neural data will likely not be covered by the Montana law because they are not in the genetic testing business.

If neural data is health or biometric information

Neural data might possibly be considered health information if an individual's health information can be derived from the neural data. Neural data might possibly be considered biometric information if an individual's identity can be derived from the neural data. If neural data is considered health information or biometric information under applicable laws, additional legal protections are afforded to such data. These additional laws would further regulate data licensing, including by imposing requirements in some additional states to obtain consent before selling or licensing such data.

Federal regulation of the sale of health information

The Federal Trade Commission (FTC) has taken actions against businesses that have sold health information to adtech companies and sensitive location information to third parties. The FTC has reasoned that consumers were not told about the sale and not given a method to decide whether their data would be included in the sale, and thus this practice was an unfair trade practice under federal consumer protection law. To date, the FTC has not applied the same rule to neural data, but it is conceivable that it would if faced with the question.

The federal Health Insurance Portability and Accountability Act (HIPAA) and the Food and Drug Administration regulations on research studies apply to neural data depending on the context in which it is collected – and the nature of the business that has collected it. If these federal laws apply, the state laws do not, but the federal laws come with their own compliance burdens. Businesses that have a choice should architect their way of doing business to either operate under HIPAA or the state laws depending on their preferred regulatory regime.

Two threshold questions: 'For free' licensing and revenue/volume gates

Before turning to the de-identification question, two questions of statutory scope cut across every one of the state regimes and are worth flagging together.

1. Does licensing data for free take you out of the regimes?

For most of the state data broker regimes, no. A purported "free" license usually does not remove the arrangement from scope. California defines "sale" broadly to include "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating" a consumer's personal information to a third party "for monetary or other valuable consideration." California courts and the state attorney general have consistently interpreted "other valuable consideration" through the lens of California's general contract law concept of consideration – any bargained-for benefit conferred on the transferor, whether or not money changes hands. In-kind exchanges of neural data for services, joint research outputs, model access or reciprocal datasets are therefore likely to qualify as a "sale." Connecticut takes a similar approach, defining "license" as granting access to or distributing personal data "in exchange for consideration" – the Connecticut statute expressly contemplates nonmonetary consideration. Vermont and Oregon both use "sells or licenses" without a narrower monetary limitation, and the market has consistently read those terms to reach nonmonetary bargained-for exchanges as well.

Texas is broader still. Its data broker definition captures any business entity that "collects, processes, or transfers" personal data it did not collect directly from the individual. "Transfer" does not require consideration at all, so even a genuinely gratuitous handoff of neural data to a third party can trigger the Texas regime (subject to Texas revenue and volume thresholds, discussed next). New Jersey uses "sells or licenses" without a defined monetary limit, and "licenses" in this context is likely to be read as encompassing noncash arrangements.

The one narrow off-ramp that runs through all of these regimes is a true one-way transfer of data with no benefit flowing back to the transferor – for example, a pure charitable donation of a research dataset to an academic institution with no reciprocal services, no access rights, no attribution and no other consideration. Companies should not assume that framing a license as "no fee" or "complimentary" removes it from scope.

2. Do the state data broker laws apply only to businesses with a certain amount of revenue or volume of data?

The answer depends materially on the state.

- **California.** The data broker regime imports the CCPA's definition of "business," which itself has thresholds – in general terms, annual gross revenue in excess of $26,625,000; buying, selling or sharing the personal information of 100,000 or more consumers or households; or deriving 50% or more of annual revenue from selling or sharing personal information. A neurotech company below all three thresholds is not a "business," and therefore not a "data broker," under the California regime. That said, the 100,000-consumer prong is easy to trip for consumer-facing neurotech, and the 50%-of-revenue prong bites hard for pure-play neural data licensors.
- **Connecticut, New Jersey, Oregon and Vermont.** No revenue or data-volume thresholds.
- **Texas.** Subject to the 50%-of-revenue and 50,000-individual thresholds described above in Model 3.

The upshot: Outside of Texas (and the narrower California "business" threshold), state data broker regimes are not size-gated. A small neurotech company licensing neural data of persons with whom it has no direct relationship can be a data broker, subject to the full compliance stack, in Connecticut, Oregon, Vermont and New Jersey. And in New Jersey, even a first-party neurotech company is regulated as a data collector regardless of size.

The de-identification question

Under every one of these regimes, data that is not identifiable to a specific person, or that has been genuinely de-identified, is out of scope. The California law excludes de-identified data from "personal information;" Connecticut's law excludes de-identified data from "personal data;" Vermont and Oregon exclude de-identified data through parallel mechanisms; and Texas has an explicit de-identification exception. The statutory standard is broadly similar across the states: The data must not be reasonably capable of being linked to an identifiable individual, and the controller must take reasonable technical measures to prevent linkage, publicly commit not to re-identify and contractually bind recipients to the same standard.

The threshold legal question for neurotech companies pursuing a licensing model is therefore whether their neural data can be de-identified to the applicable legal standard. That question is not settled. Reasonable technical experts disagree. What follows is the best case for each position.

The argument that neural data can be de-identified (and data laws therefore do not apply)

The strongest argument that neural data can be adequately de-identified runs through a simple fingerprint analogy: A fingerprint lifted from a crime scene identifies no one on its own. It becomes identifying only when a fingerprint database exists and the lifted print can be matched against it. Neural signatures work the same way. A neural signal "lifted" from an anonymized dataset can identify a specific individual only where a reference database exists that ties known individuals to their neural signatures. That kind of reference database does not exist today for the general population, and in most licensing scenarios it does not exist for the licensed-out population either. Where the reference set does not exist, the neural signal cannot be linked to any particular person as a matter of fact, regardless of how unique it is in theory. If the reference set does exist, but is not accessible to the entity that holds the neural data, then the neural data is not identifiable from that entity's perspective.

The statutory standards support this reading. Connecticut requires that the data "cannot reasonably be used to infer information about, or otherwise be linked to," an identifiable individual. The CCPA requires that the data "cannot reasonably be used" to identify or associate with a consumer. Both standards are grounded in reasonableness, and reasonableness is calibrated to the state of the world today, not to speculative future capabilities. If linking a neural signal to a person requires access to a reference dataset that no one has built for the population in question, the linkage is not reasonably available, and the data satisfies the statutory de-identification test.

The technical picture also cuts more finely than the skeptics allow. Neural signatures are not stable in the way that traditional biometrics are. A fingerprint is essentially fixed for life; a neural signature varies with sleep, mood, attention, age, medication and disease state. The high identification accuracy rates in the research literature are typically achieved within a single session and cohort, on high-fidelity recordings, using algorithms tuned to the specific data. Licensed-out neural datasets can be downsampled, aggregated, cropped to short windows or transformed into derived features that discard much of the individuating detail.

In practice, de-identification measures can combine several techniques at once: removing hidden identifying tags from files (metadata scrubbing), reporting group-level figures instead of individual records (aggregation), adding small amounts of random "static" to obscure exact values (statistical noise), ensuring each described group is large enough that no one person stands out (k-anonymity-style controls), and dropping unusually rare records that would be recognizable on their own (outlier suppression). And where the underlying data is already coarse to begin with – for instance, a summary index (such as an attention or workload score) rather than a raw, moment-by-moment brain signal – the remaining risk of identifying a person can be substantially lower, and in some cases may fall below what the applicable law counts as personal or neural data.

The statutory de-identification standard also depends on business controls that neurotech companies can and do implement. Public commitments not to re-identify, contractual undertakings from downstream recipients, technical safeguards against linkage and monitoring for compliance are all feasible in commercial licensing arrangements. Where those controls are in place and the underlying data is not intrinsically identifying to the population in question, it can be said that the data satisfies the statutory de-identification test, or that it was not identifiable to start. In short, the de-identification off-ramp is available for neural data – it just requires a defensible technical basis and disciplined contractual architecture, not a blanket assumption.

The arguments that neural data cannot be de-identified (and data laws therefore apply)

The identifiability skeptics rest on a growing body of neuroscience research suggesting that neural signatures function as biometric fingerprints. A widely-cited 2015 fMRI study identified individuals from their whole-brain functional connectivity patterns with 93 – 94% accuracy in cohorts drawn from the Human Connectome Project (Finn et al., Functional Connectome Fingerprinting: Identifying Individuals Using Patterns of Brain Connectivity, 18 Nature Neuroscience 1664 (2015)). Each target scan was matched to the most similar entry in a database of prior scans from the same subjects, so the result speaks to the risk of linking a new scan to an existing record rather than to identification from a neural recording alone.

A 2014 EEG study achieved 100% accuracy in matching people to their brain recordings by looking at how different parts of the scalp "talked to" one another at specific frequencies, rather than at any single sensor on their own (La Rocca et al., Human Brain Distinctiveness Based on EEG Spectral Coherence Connectivity, 61 IEEE Transactions on Biomedical Engineering 2406 (2014)). As with the fMRI work described above, that accuracy was measured against a closed reference set – each new recording was matched to the most similar entry in a database of prior recordings from the same people – so the result speaks to the risk of linking a new scan to an existing record rather than to identifying a stranger from a brain recording alone. Later reviews of the EEG-identification literature report similar or slightly lower accuracy figures, typically in the high-80s to high-90s, across a range of methods and datasets.

And identification does not require long recordings. A 2021 MEG study reported that just thirty seconds of resting-state brain activity was enough to correctly pick a participant out of a closed cohort roughly 84% of the time – compared with about 95% when longer segments were used (da Silva Castanheira et al., Brief Segments of Neurophysiological Activity Enable Individual Differentiation, 12 Nature Communications 5713 (2021)).

There is also a distinct identifiability pathway that has nothing to do with neural fingerprinting. In speech and communication brain-computer interfaces (BCIs), the decoded output is not a signal signature but the user's own words. Everyday speech and messaging routinely surface autobiographical detail – the speaker's own name, references to family members, an employer or workplace, a medical diagnosis, or other personal facts – that identifies the person on the face of the transcript, without any comparison to a reference dataset. For that class of neural product, the identifying information is embedded in the content itself.

That distinction – between recognizing someone by the pattern of their brain activity and identifying them from what they said – is one instance of a broader point that the current debate tends to skip past: Not all "neural data" is the same thing, and different forms of it carry very different re-identification risk. A raw recording taken directly from the electrodes; a set of summary measurements calculated from that recording (for example, how much activity is present in different frequency bands, or how strongly different brain regions move together); the

trained software model that translates brain activity into speech, movement or a category label; the decoded output itself (the actual text, speech or cursor movement the system produces); and a high-level conclusion drawn from the data (for example, a single "alertness" or "focus" score) each sit at a different point on the identifiability scale, even when they all come from the same recording session. What is enough to strip identifying information out of an alertness score will not be enough for a raw recording, and the reverse is equally true. The same regulated term – "neural data" – is doing very different work as the information moves through these stages, and any workable de-identification analysis has to look at the specific form at issue, not just at the category label.

The intrinsic uniqueness of neural data has three consequences under the statutory de-identification tests. First, small datasets are trivially re-identifiable within their own populations: A neurotech company holding neural recordings from 200 research subjects may be able to associate neural data with specific individuals without any external reference. Second, reference datasets are actively being built. Large-scale consumer neurotech products, invasive BCI companies and academic-industrial collaborations are generating neural datasets at scale, and open science initiatives are publishing sizable reference corpora, which means that even a "bare" neural sample that is not identifying today may be identifiable tomorrow through comparison to a growing reference base. Third, neural data reveals sensitive attributes – cognitive state, health conditions, emotional response profiles – that themselves can be linked with other data to re-identify a specific person, especially in small populations with distinctive clinical characteristics.

Finally, the regulatory apparatus is unusually demanding on the de-identification side. It requires reasonable technical measures to prevent re-identification, a public commitment not to re-identify, contractual downstream controls that flow those obligations to every recipient and ongoing monitoring of the recipient's compliance. Neural data licensing arrangements need to be designed to meet those requirements in practice, particularly the downstream contractual and monitoring components. On the other hand, under the California law for example, if data de-identification has rid a business of any of the personal identifiers that consumers can use to request data brokers to delete their data, such as email addresses and phone numbers, the data broker will be hard-pressed to delete data even in the face of a deletion request, possibly making it impossible for the business to comply with the law.

Where this lands

Reasonable minds will continue to differ, and the answer for any particular licensing arrangement is fact specific. It depends on the type of neural data – identification accuracies vary meaningfully across modalities, and EEG, fMRI, MEG and fNIRS each carry different identifiability profiles even before considering feature engineering, so the answer for a raw EEG recording is not the answer for a downsampled fMRI feature vector. It also depends on the amount of neural data per subject. The size and distinctiveness of the licensed-out population, the availability of a reference dataset that could support linkage, and the technical and contractual architecture the licensor puts around the data round out the analysis. What is clear is that a blanket "we'll de-identify" strategy is not a substitute for the analysis. Companies pursuing a de-identification path should pressure-test it with both technical experts and privacy counsel – dataset by dataset, modality by modality and duration by duration – and paper the required public commitments, contractual controls and monitoring practices before treating the licensed data as out of scope.

A note on the parallel state consumer privacy law regimes

Separate from the state data broker registration laws discussed above, the sibling comprehensive state consumer privacy laws in 23 states will apply independently to any business that qualifies as a "controller" of neural data, and meets the triggering metrics of the law, meaning a business that (alone or jointly with others) determines the purposes and means of processing that neural data. "Processing" in each of those statutes is defined broadly to include the collection, use, storage, disclosure, sale and licensing of personal data, so licensing neural data downstream is a processing activity that a controller performs. Controllers of neural data are subject to notice, consent, purpose-limitation, minimization, sensitive-data opt-in and data protection assessment obligations under those laws (subject to the state-by-state applicability thresholds), regardless of whether the business is also a "data broker" under the state's data broker regime. In short, a neurotech company that stays below a data broker regime's coverage line can still be a controller of neural data subject to the parallel privacy law's substantive obligations.

Practical takeaways for neurotech companies

1. **Map your data flows against each state's definitional model.** Identify every neural dataset your company licenses, sells or grants access to, and separate them into datasets about individuals with whom you have a direct contractual or similar relationship and datasets about individuals with whom you do not. Also, identify the states of residence of the individuals whose neural data is to be licensed, so that the applicable laws' requirements can be met.
2. **Do not rely on de-identification as an off-ramp without stress-testing it.** Confirm the type of neural data you are licensing, the size and distinctiveness of the licensed-out population, whether a reference dataset exists (or is plausibly being built) that could support linkage, and whether your technical and contractual controls meet the applicable statutory standards. Paper the public commitments and downstream contractual undertakings the statutes require.
3. **Choose your regulatory regime.** If your business has a choice between HIPAA and the state data law regime, examine both carefully, choose which regime best meets your data needs, and architect your way of doing business to fit into, and comply with, your preferred regulatory regime.

Key Contacts

Kristen Mathews **New York**	**kmathews@cooley.com**