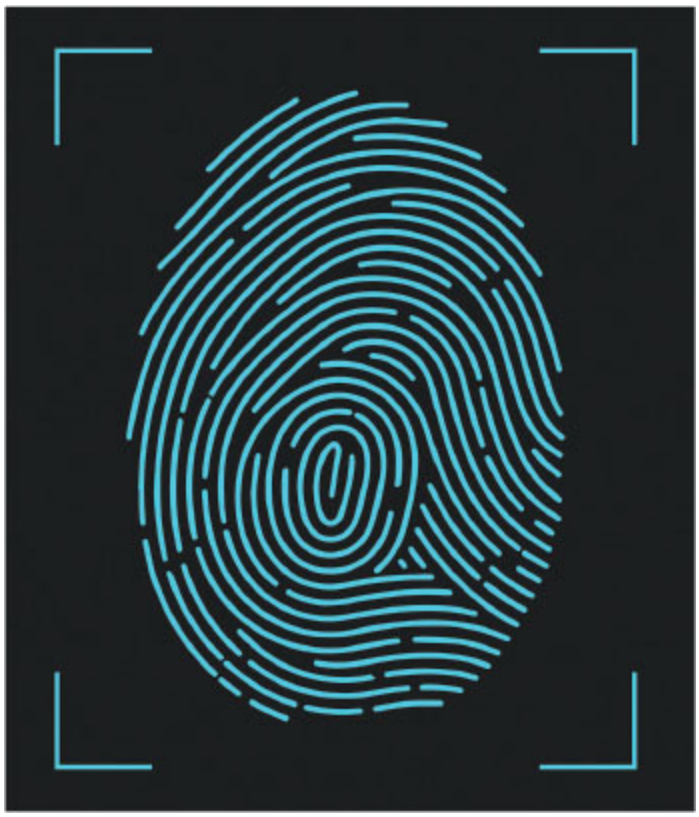
August 2025

Your Biometrics Briefing

As state governments enact laws regarding the collection, dissemination and deletion of sensitive data, it's increasingly important to ensure your firm is operating within its legal bounds.

BY WENDY WIENER, LAUREN R. PETTINE AND HENRY THOMPSON



Over the past decade, state legislatures and the courts have become more concerned with protecting individuals' privacy and data. A handful of states have enacted laws that govern personally identifiable information (PII), biometric data or both. These laws mandate consent from impacted individuals and regulate the collection and use of the information by businesses such as yours.

Why are we, deathcare professionals, concerned with the collection and use of PII and biometric data now? Prior to the 1980s, large databases of information about

and biometric data now? Prior to the 1980s, large databases of information about consumers and decedents were not generally accessible. Now, however, it's commonplace for databases of consumer information to be sold for commercial purposes. It also is commonplace for such databases to be breached. Who hasn't received a text, email or letter informing them of a data breach or inviting them to participate in a data-related class action?

Deathcare licensees come into possession of data related to decedents and other persons and, as a result, are and may be subject to the relevant laws. Of even greater concern is the number of burgeoning lawsuits – and one class action – brought against funeral homes by family members of decedents from whom biometric data was collected without permission.

In the paragraphs that follow, we will unpack the impacts of new (and not-so-new) laws relating to PII and biometric data, and provide you with best practices to keep your data and your business from becoming targets of regulators and lawyers.

WHAT IS PROTECTED DATA?

Let's start with an orientation. There are two kinds of sensitive information with which deathcare licensees are likely to come into contact. Those are personally identifiable information (PII) and biometric data. PII is data, including names, social security numbers, financial information such as credit card numbers, e-mail addresses, phone numbers, physical addresses and dates of birth, that can be used to identify, locate or contact a specific individual,. Biometric data pertains to unique physical characteristics that can be used to identify or verify the identity of an individual. Biometric data relies on features that are inherent to each individual, such as fingerprints, facial recognition and DNA.

REGULATIONS

States primarily regulate the collection and dissemination of biometric data through Biometric Data Privacy Acts. We'll call this kind of law a BDPA. In contrast, PII is often regulated by a state's Consumer Privacy and Protection Act (CPPA). As of the date of this writing, Colorado, Illinois and Texas have both a BDPA and CPPA. Washington has a BDPA. And three states – Nevada, North Carolina and Oregon – have enacted a CPPA that is broad enough to cover biometric data. Put

Oregon – have enacted a CPPA that is broad enough to cover biometric data. Put more simply, seven states have enacted laws that address biometric data to some degree.

These two kinds of acts differ in multiple ways. In most cases, CPPA laws apply only to living individuals. For example, this would include customers who purchase a funeral, attend a funeral, leave a comment on an online obituary or receive a newsletter from a funeral business. Courts have found that usually only living consumers have a privacy right. You might have heard that "privacy rights die with the decedent." Well, that's why. In contrast, BDPA laws may apply to decedents in the care of deathcare licensees. Although some BDPA laws are written to expressly cover decedents, most BDPA laws are silent as to whether the protections apply to an individual after death. In that case, though, silence is not a pass to disregard the requirements of the BDPA. You'll read later about litigation involving biometric data that is pending in Florida, a state that doesn't even have a BDPA.

Of course, deathcare licensees come into contact with individuals who are living and deceased and, therefore, may be subject to the requirements of CPPAs and BDPAs. Both laws regulate consent, collection, use and deletion of data.

COLLECTION AND CONSENT

For both forms of data, consent of the individual or the individual's agent is *required* (note our emphasis – more on that later) in order for a business to collect the relevant data. This consent must be explicit. In most cases, the consent form for this authorization must expressly describe the policies regarding the collection, use and retention of the data in question. For PII, the consenter also may require either dissemination or deletion of the data upon request.

For instance, the Illinois Biometric Information Privacy Act, passed in 2008, requires that the written authorization, executed prior to the collection of biometric data, incorporate a variety of information. This information includes confirmation that the biometric data is being collected, the length of time for which the data will be stored, a description of the intended use of the data and the data retention policy. We call attention to the Illinois law because it's the alleged violation of this law that is the basis for an ongoing class action against

three Illinois funeral homes and Legacy Touch Inc., a fingerprint keepsake company. The lawyer for the families seeks to expand the lawsuit to class action status, which would include every family of a decedent from whom Legacy Touch and the funeral homes collected biometric data in Illinois as members. In our opinion, if successful in Illinois, the lawsuits likely will not stop there.

We have long recommended that our clients obtain authorization prior to the collection of biometric data (e.g., fingerprints, locks of hair, DNA samples, etc.) or photographs. Ideally, authorization is customized to address the requirements of the state where the licensee is located, and if there are no current requirements for the given location, then the authorization form aligns with the most restrictive state's law. The form developed for use in Illinois provides required information to the authorizing agent and captures authorization(s) in writing. Any document used for this purpose also must permit an individual to refuse the collection of biometric data.

USE AND DISSEMINATION

These laws also govern the dissemination of PII and biometric data. This means that if PII or biometric data is released to other parties, such as keepsake or DNA analysis companies, the authorizing agents and consumers must consent specifically to the delivery of the biometric data to such companies for those purposes.

Washington's BDPA prohibits enrolling a biometric identifier in a database for a commercial purpose without first giving notice, obtaining consent or providing a mechanism to prevent the subsequent use of the biometric data for a commercial purpose.

Additionally, most states with a BDPA require that the biometric data is protected by the holder of said data in specific ways. For instance, businesses that obtain biometric data in Colorado are required to establish internal protocols for responding to incidents that compromise the security of said data. Companies in possession of PII and biometric data should be certain of the security of that data and take reasonable industry-standard measures to protect it. Your IT department or contractor must be your partner in ensuring that all sensitive data vou collect and retain is secure.

> ***Of even greater concern is the number of burgeoning lawsuits – and one class action – brought against funeral homes.***

Your collection authorization form is a good place for explicit statements regarding your intended release of information. On the form, address the purpose of the release and describe your retention policy, including for how long the data will be retained. If your state's BDPA is comprehensive, you may be required to identify the company to which the data will be released. All of these requirements are met easily with the use of a robust form.

DELETION

The laws sometimes state that businesses collecting PII or biometric data must have a deletion or retention policy. Such a policy requires that you review and delete the data after a certain period. Generally, in states with such a BDPA, you may not retain decedents' fingerprints, photographs or DNA indeflnitely.

Your company policy should dictate that covered data will be deleted after a time certain. In fact, in some states, such as Illinois, this is a legal requirement. In Illinois, the BDPA mandates the establishment of a schedule and guidelines for permanently destroying biometric data. Illinois law requires that biometric data be deleted either three years after the individual's last interaction with the private entity or once the reason for the data collection has been satisfied – whichever occurs first. Colorado's 2025 Biometric Data Privacy Act states each company that acquires biometric data must have a written retention schedule for the deletion of biometric identifiers. Dependent on which happens first, deletion must occur on or before the date upon which the initial purpose for collection is satisfied or within two years of the individual's last interaction with the business. This retention policy must be made available to the public and accessible to consumers.

> ***Licensees come into contact with individuals who are living and deceased and … may be subject to the requirements of CPRAs and BDPAs***

and … may be subject to the requirements of CPPAs and BDPAs.

Licensees should have a deletion or retention policy that allows consumers to request that PII or biometric data be deleted and that dictates PII and biometric data are periodically deleted from their records. Your authorization form is, again, a great vehicle to use to make the family aware of your retention policy.

WHAT'S NEW IN STATE AND FEDERAL REGULATION?

This is a fast-evolving area of the law. As of this writing, 20 states have enacted consumer data privacy acts, but only seven have laws that could be read to expressly cover biometric data. Notably, Florida, Kentucky, Maine, Massachusetts, Minnesota, Missouri, New York and other states have contemplated developing biometric data laws.

Additionally, the federal government has become more concerned with the security and use of biometric data. In May 2023, the Federal Trade Commission (FTC) created a policy statement regarding the use of biometric information and its regulation under Section 5 of the Federal Trade Commission Act.

This policy statement advises that false claims about the accuracy or efficacy of biometric information technologies or false claims about a business's collection and use of biometric data may violate the act. The FTC considers several factors when determining whether a business has violated the act, including:

1. Failing to assess foreseeable harms to consumers before collection of biometric information
2. Failing to address known or foreseeable risks and identify and implement tools for reducing or eliminating those risks
3. Engaging in surreptitious or unknown collection or use of biometric data
4. Failing to evaluate the practices and capabilities of third parties such as affiliates, vendors or end users that will be given access to biometric data
5. Failing to provide appropriate training for employees or contractors who come into contact with biometric data

6. Failing to provide ongoing monitoring of technologies that use such information and ensure that technologies are functioning properly and avoiding harm to consumers

To translate the legal jargon: When determining whether a violation of the act has occurred, the FTC looks at whether a business, such as a funeral establishment, recognizes and appreciates the risk of collecting biometric data and trains its employees to ensure the safety of such data. Having solid consent procedures – and an authorization form – will help keep businesses safe from potential FTC action.

Violations of the seven existing biometric privacy laws come with stiff fines. Illinois law provides that a person whose data is impacted will have a private right of action to collect $1,000 per violation and either $5,000 or actual damages, as well as attorneys' fees and costs. Other states, such as Washington and Texas, do not permit a private cause of actions for individuals but instead permit their attorneys general to investigate and punish violators of the BDPA.

BIOMETRIC DATA IN THE COURTS

ILLINOIS CASE

As we touched on before, in Illinois, Legacy Touch Inc. and three funeral homes were sued for collecting and using decedents' fingerprints for commercial gain. Currently, Legacy Touch Inc. and one funeral home remain defendants in the proposed class action. According to court papers, the funeral homes, at the direction of Legacy Touch, collected fingerprints of decedents without permission and provided those fingerprints to Legacy Touch for the purpose of selling keepsakes. The lawsuit alleges that Legacy Touch, which advertises keepsakes and jewelry using the fingerprints of individuals, did not have adequate consent forms for this practice. The lawsuit contends that Legacy Touch encourages funeral homes and cremation facilities to collect fingerprints without the knowledge or prior express consent of authorizing agents. Because consumers were not informed about the specific purpose of the fingerprints and because of the collection, storage and use of said fingerprints, the plaintiffs pray for damages that could exceed $5 million if the class is certified.

FLORIDA CASE

FLORIDA CASE

In Florida, another case naming a funeral home owner/operator and Legacy Touch Inc. was settled recently. The claims made (by the same lawyer involved in the Illinois case, by the way) are nearly identical to those in the Illinois class action: failure to secure permission prior to collection and use of decedents' biometric data. The case, which had been ongoing for some time, prompted Florida legislators to attempt to pass a law that would specifically regulate the use of biometric data by funeral homes. The law did not pass, but we expect to see it put forward year after year, and if/when it passes, it will be the first law in the country to specifically target deathcare. Florida's chief financial officer, the ultimate regulator of funeral homes in Florida, has stated that the Department of Financial Services recommends all funeral establishments obtain permission from a legally authorized person before taking the fingerprints of a decedent for any purpose.

BEST PRACTICES

OK, WE'RE SCARED! NOW WHAT?

Fear not. You can continue to ofter keepsakes that utilize biometric data, collect DNA samples upon request and to sell for analysis, and take photographs of decedents when necessary, so long as you implement and follow some best practices.

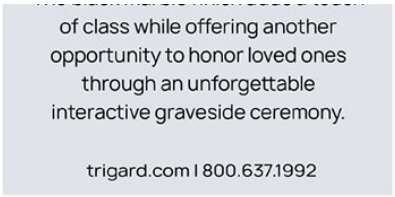
1. Create or obtain an authorization form, then use it. We mean, secure authorization before you collect biometric data from a decedent.
2. Make sure the form complies with your state's BDPA requirements. Because there are only a few such laws in effect as of this writing, most of your authorization forms will be more generic, but they still should contain:
    - Explicit authorization to collect whatever you are collecting
    - A description of what you will do with the collected biometric data and the name of the company to which the data will be released
    - A description of how the biometric data will be stored

- A date/time by which you will destroy the biometric data (*Note: We recommend destroying biometric data two years after collection. This is the shortest time frame set forth in law so far. That way, there's no possibility of retaining data for too long*.)

3. If you provide biometric data to a third party (keepsake creator, DNA analysis company, etc.), obtain the third party's storage and retention policy. If it's different than yours, have the company confirm it will comply with your policy.

Seven laws are on the books, and there are certainly more to come. Be prepared. We've got a form – do you?

The lawyers of WRW Legal PLLC, led by Managing Member Wendy Russell Wiener, who has 33 years of deathcare regulatory experience, focus their practices solely on guiding the owners, operators and professionals of funeral homes, cemeteries and crematories. They practice law in Florida and ofter regulatory compliance guidance in 30-plus other states.



at the 2025 NFDA Convention for an up-close look!

The black marble finish adds a touch of class while offering another opportunity to honor loved ones through an unforgettable interactive graveside ceremony.

trigard.com | 800.637.1992