



## Beyond life

### FROM APPLE WATCHES AND FITBITS TO OURA RINGS, THE ROLE OF WEARABLE HEALTH METRICS IN SURVIVAL ACTIONS AND OTHER PI LITIGATION

As wearable health technology becomes increasingly integrated into daily life, its role in the courtroom is rapidly expanding. Devices like Apple Watches, Fitbits, and Oura Rings now generate continuous biometric data, heart rate, sleep cycles, and physical activity that may offer powerful evidence in personal injury litigation. In California, this evolution is particularly timely. Historically, California restricted recovery of pain and suffering in survival actions, the claims pursued by an estate after the injured person's death. However, the 2022 amendment to Code of Civil Procedure section 377.34 now permits recovery for pain and suffering in survival actions, raising new possibilities, and concerns, for how biometric data might be used to prove damages, especially when the injured party is no longer alive to speak for themselves.

#### Legal evolution of pain-and-suffering damages

Previously, non-economic damages were limited to living plaintiffs. This left estates unable to recover for a decedent's pain and suffering experienced before death. Courts acknowledged the unfairness of this restriction, especially when individuals endured significant suffering shortly before passing. The 2022 amendment addresses this inequity, authorizing estates to recover for pre-death non-economic harm. Consequently, courts will have to determine whether objective sources like wearable data is admissible to assess pre-death damages.

California courts, prior to this amendment, faced difficult decisions. In cases such as *County of Los Angeles v. Superior Court (Schonert)* (1999) 21 Cal.4th 292, courts recognized documented suffering but denied damages due to the legal framework. Now, with a statutory foundation supporting pain-and-suffering recovery, judges are more empowered to consider wearable digital evidence, including health data collected outside traditional medical settings.

This legislative change also harmonizes California law with broader national discussions on equitable access to justice for decedents. By recognizing the value of subjective harms, pain, fear, loss of dignity, through objective tools like biometric data, the amendment creates a modernized evidentiary bridge between lived experience and legal remedy.

#### Privacy rights and posthumous protection gaps

While laws like the Health Insurance Portability and Accountability Act ("HIPAA") and the California Consumer Privacy Act ("CCPA") protect health data, these protections are incomplete. HIPAA excludes most wearable tech companies as they are not "covered entities," and the CCPA does not expressly cover the data of deceased individuals. As a result, biometric data from wearables often falls into a legal grey zone. The California Privacy Rights Act ("CPRA") enhanced protections for living individuals but still does not address who controls or accesses data after death. This gap poses challenges when wearable data is crucial to survival-action litigation but raises unresolved questions about privacy, ownership, and consent.

The Ninth Circuit's decision in *Marsh v. County of San Diego* (9th Cir. 2012) 680 F.3d 1148, highlighted the importance of familial privacy regarding a deceased individual's remains and sensitive information, suggesting that courts are open to recognizing posthumous privacy interests. Nevertheless, without clear legislative direction, such recognition remains limited.

Further complicating this issue is the nature of data ownership. Unlike traditionally controlled by healthcare providers, wearable health data may be stored by private tech companies and governed by opaque user agreements. This creates ambiguity for estate representatives seeking to access such data in litigation.

HIPAA, while providing 50 years of protection for personal health information post-death, does not govern data collected by most wearable technology companies, since they do not qualify as "covered entities." As a result, HIPAA does not apply to health data generated by Apple Watches, Fitbits, or Oura Rings, leaving a large volume of posthumous biometric data outside the scope of federal privacy protections. State law thus becomes critically important. The CCPA and its expansion through the CPRA attempt to fill this gap.

The CPRA introduced new data protection standards. Among its most impactful features is the recognition of "sensitive personal information," including biometric and health-related data. Under CPRA implementing regulations (Cal. Code Regs., tit. 11, §§ 7002-7028) businesses must limit data collection to what is necessary and proportionate. Additionally, section 7050 requires service providers to use data only for specified purposes and to notify companies when they can no longer comply. (Cal. Code Regs., tit. 11, § 7050.)

Still, despite its advancements, the CPRA fails to address posthumous privacy directly. It does not establish who has control over sensitive data after death, how long companies can retain it, or whether it may be accessed in litigation. As courts increasingly look to wearable data to substantiate legal claims, this statutory silence creates uncertainty for families, litigants, and companies alike.

Case law adds further nuance. In *Carpenter v. United States* (2018) 585 U.S. 985, the U.S. Supreme Court recognized that individuals have a reasonable expectation of privacy in digital location data held by third parties. Although *Carpenter* was a criminal case, its privacy rationale suggests courts may similarly protect the integrity of posthumous digital data in civil actions, especially when sensitive biometric indicators are involved.

### Judicial approaches to wearable health data

Courts are increasingly admitting wearable data to evaluate claims. In *Bartis v. Biomet, Inc.* (E.D.Mo. 2021) No. 4:13-CV-00657-JAR, 2021 WL 2104986, Fitbit data was used to measure a plaintiff's mobility post-injury. In *State v. Dabate* (Conn.Sup.Ct. Apr. 27, 2017) No. TTD-CR17-0110576-T, 2017 WL 1416810, similar data was admitted in a criminal case to establish a timeline. While courts often find wearable data admissible under rules like Federal Rules of Evidence, rule 401 and 702 or Evidence Code, sections 1400 and 352, admissibility also hinges on authentication, relevance, and expert interpretation.

However, wearable data must be contextualized. Elevated heart rates may indicate pain or may reflect unrelated stressors. Without expert testimony, such data can be misleading. Courts must ensure biometric signals are tied to the claimed injuries and not external factors. Without such safeguards, there is a risk of overinterpretation, especially in emotionally charged cases where juries may place undue weight on technological data.

Courts have also shown reluctance to admit wearable health data in the absence of clear chain of custody or scientific reliability. Under *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (1993) 509 U.S. 579 and related California standards, data introduced must be both relevant and reliable. If wearable data cannot be authenticated through expert testimony or device-specific validation, it may be excluded.

### Ethical and practical considerations

Admitting wearable data also raises ethical issues. Most users don't expect their devices to generate posthumous litigation evidence. Families may experience emotional harm from data revealing a loved one's suffering. Moreover, courts risk over-relying on data that is correlational, not causal. To address these concerns, courts should explore clear consent frameworks and expert interpretation.

Technological literacy also matters. Judges and jurors may lack the expertise to interpret biometric data accurately. Litigants with greater technical resources may gain unfair advantages. Procedural safeguards and disclosure requirements, such as motions in limine or expert witness mandates, are crucial. There are also practical issues surrounding the chain of custody, storage, and interpretation of data over time. Without robust protocols, data risks being altered, misused, or misunderstood. In criminal and civil proceedings alike, courts have been wary of admitting data that lacks adequate documentation regarding who had access to the data, when it was extracted, and how it was analyzed.

Furthermore, consent for posthumous use remains murky. Most terms of service agreements do not specify what happens to user data upon death, leaving survivors, courts, and litigants in uncertain territory. This raises the question: Should wearable device manufacturers be required to offer settings that allow users to specify how their data may be accessed or used after death?

### Proving pain and suffering through wearable data

The amendment to Code of Civil Procedure section 377.34 opens the door for estates to use wearable data to prove non-economic damages. For instance, a declining activity pattern before death may support claims of suffering, while the absence of distress signals might challenge such claims.

Yet biometric data must be supported by expert testimony to ensure reliability. Medical professionals may be required to interpret whether elevated physiological readings, like sustained heart rate spikes or disrupted circadian rhythms, are consistent with physical pain or emotional trauma. Such interpretations must be grounded in medical literature and data science principles to ensure fairness and avoid speculative conclusions.

Courts must develop evidentiary standards for wearable data. This includes chain-of-custody requirements, device

reliability verification, and analysis transparency. Without these measures, courts risk inconsistent rulings and privacy violations.

These evidentiary standards should align with both state and federal norms. Under *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, (1993) 509 U.S. 579 federal courts require expert testimony to be both relevant and scientifically reliable. California applies a similar standard under the *Kelly/Frye* framework, requiring a foundational showing that the scientific principle is generally accepted in the relevant scientific community. For wearable health data, this means litigants must not only demonstrate that the device is accurate and functioning properly but also provide expert interpretation of what the data actually means.

#### Expert testimony

Expert testimony is particularly important when data must be interpreted contextually. For instance, a sudden drop in physical activity may be attributed to pain or injury, but could also result from unrelated causes like medication side effects or temporary illness. Without expert guidance, triers of fact may draw inappropriate inferences from biometric fluctuations. Experts also need to explain device-specific considerations such as battery level, device placement, user compliance, and firmware version, all of which can affect data quality.

For example, a wrist-worn heart rate monitor may be highly accurate when worn properly, but show significant deviations if worn loosely or during vigorous movement. Experts must help courts navigate these technical nuances to avoid overreliance on incomplete or misleading data.

In addition, courts may benefit from transparency about the proprietary algorithms used by device manufacturers. Since these algorithms often determine how raw data is translated into user-facing metrics (e.g., sleep stages or activity scores), litigants should be prepared to disclose whether the algorithm has been peer-reviewed, validated, or changed during the

relevant time period. Courts could require disclosures about firmware updates and algorithmic logic to assess whether the device's data remains stable and scientifically sound over time.

### **Toward a posthumous data-protection framework**

To responsibly govern wearable data, California must establish legal clarity around posthumous data ownership and consent. Legislation should empower individuals to decide, in life, whether their wearable data can be used posthumously and for what purposes. Device manufacturers should also be held to clear standards on data retention, disclosure, and user control.

Manufacturers could be required to implement user settings allowing individuals to specify preferences for data use after death. Much like an advance healthcare directive, such "digital directives" would offer clarity for families and courts alike. Additionally, courts should consider limiting admissibility of posthumous wearable data to instances where it serves a compelling interest and where alternative sources of evidence are unavailable.

Legislatures may also consider a probate-style mechanism to allow estates to contest the use of biometric data before it is admitted in court. Another potential reform involves requiring companies to maintain posthumous access logs or consent registries, ensuring estate representatives can access necessary data only under verified, lawful conditions.

Procedurally, courts may rely more heavily on motions in limine and protective orders to govern the admissibility of wearable data. These pretrial tools can help balance the probative value of biometric evidence against potential prejudice or emotional harm, particularly in cases involving graphic physiological indicators of pain or death. A carefully tailored motion in limine could, for example, limit the scope of admissible data to specific time windows or metrics directly relevant to the injury in question. Together, these procedural innovations could bring much-needed structure to a

rapidly evolving evidentiary landscape and promote consistent, ethically sound outcomes in future litigation. This approach could protect both individual dignity and judicial integrity.

### **Digital dignity and the legacy of consent**

Courts have long recognized that legal protections do not end at death. From defamation law to probate proceedings, our legal system has historically acknowledged a decedent's reputation, wishes, and dignity. The posthumous use of wearable health data intersects directly with these traditions, challenging the legal system to balance evidentiary access with respect for the deceased.

Ethically, this debate mirrors the longstanding medical principle of informed consent. Just as patients must authorize the use of their medical records, individuals should have the opportunity to specify how their biometric data is used after death. Failure to honor these decisions not only undermines personal dignity but may also deter individuals from embracing health technology in life due to concerns about posthumous data misuse.

The CPPA, as the state's primary regulatory body for digital privacy, is uniquely positioned to lead in this area. By issuing interpretive guidance or proposing regulations that address posthumous biometric data, the CPPA could provide clarity and leadership where statutory silence has persisted. Such guidance could include default data retention timelines, authorization forms for estate representatives, and model disclosures for wearable device terms of service.

### **Expanding the evidentiary frontier**

In practice, wearable health data also opens up broader questions about the future of tort litigation. Courts and litigants are increasingly navigating a shift from narrative-based evidence to real-time, digital documentation. As legal scholars have noted, the evidentiary weight of biometric data may ultimately

influence how pain, suffering, and emotional distress are argued and understood in court.

This technological integration could also affect settlement dynamics. Defendants may seek access to a decedent's wearable data early in discovery to evaluate exposure to pain-and-suffering damages, while plaintiffs may use the same data to substantiate high-value claims.

As courts grow more accustomed to such evidence, there may be pressure to develop clearer procedural pathways for litigating data-heavy survival actions. The role of forensic experts, particularly those with combined expertise in medicine, engineering, and data analytics, will become more central. These experts not only translate biometric patterns into comprehensible legal narratives but also help courts understand the reliability and scope of the data being offered. Their input may shape jury instructions, evidentiary rulings, and even appellate review in this rapidly emerging space.

### **Ensuring evidentiary balance in the age of biometrics and bridging evidentiary gaps**

In addition to supporting plaintiffs, wearable health data can serve as a powerful tool for defendants to challenge exaggerated or unfounded claims. For example, if a decedent's device shows consistent activity, normal sleep, and stable vitals in the days leading up to an alleged decline, this may undermine claims of prolonged suffering. The empirical nature of biometric data introduces a form of accountability that benefits all parties by anchoring arguments in documented fact. Courts should encourage the use of such data not only to prove claims, but to test them as well.

Looking beyond California, few states have squarely addressed posthumous biometric data in their privacy laws. However, some have moved toward expanded definitions of personal data. Illinois, for example, has the Biometric Information Privacy Act ("BIPA"), which includes strong protections for biometric identifiers.

Although BIPA does not address posthumous data, it reflects a legislative willingness to engage deeply with biometric privacy. California's CPRA could follow suit by adding provisions specifically governing access and use of biometric data after death.

As California continues to lead in privacy and technology policy, a strong framework for wearable data in litigation should include four key components:

- (1) statutory clarity on posthumous data ownership and consent;
- (2) procedural mechanisms for evidentiary disputes;
- (3) transparency obligations for device manufacturers; and (4) educational initiatives to equip courts with the tools needed to evaluate biometric evidence.

### **Upholding posthumous dignity through statutory clarity**

Ultimately, the legal treatment of wearable health data after death must reflect both evidentiary fairness and enduring principles of privacy and dignity. As personal-injury litigation continues to evolve alongside digital health innovations, California stands at a pivotal moment. Statutory reforms that explicitly define posthumous consent, data ownership, and the evidentiary

boundaries of biometric material are no longer optional, they are essential. By taking deliberate steps to modernize its legal infrastructure, the state can preserve both the integrity of its courts and the rights of those no longer here to defend themselves.

### **Conclusion**

California's recent legal shift allowing pain-and-suffering damages in survival actions presents both opportunity and challenge. Wearable data offers a promising evidentiary tool to quantify non-economic harm, but its use must be tempered by rigorous legal, ethical, and privacy standards. To ensure justice and dignity, courts and lawmakers must work together to create a coherent framework governing the posthumous use of biometric data in litigation.

*Siran Keosian graduated from Loyola Law School with a Juris Doctor degree in the spring of 2025. She received her undergraduate degree from the University of Southern California.* 