
THE EVIDENTIARY STATUS OF WEARABLE HEALTH DATA: ADMISSIBILITY, AUTHENTICATION AND THE LIMITS OF RELIABILITY IN CONTEMPORARY LITIGATION

Paritosh Panda, Sambalpur University

ABSTRACT

Fitness trackers, smart watches and biometric rings are now on the market that can keep continuous, detailed records of heart rate, sleep, where and how you're moving. Users and investigators across different continents have started to submit this data to provide timelines, support or disprove evidence, and to quantify the injury, but there is no jurisdiction to have developed an evidentiary regime specifically for wearable data, courts take existing rules for business records, expert testimony, and general electronic evidence and apply them to a technology with proprietary sensors, opaque algorithms, and dubious accuracy, even from the makers. The article examines how wearable health data is admitted as evidence in the United States, the European Union and India, analyzing the evidentiary mechanisms by which wearable data gets in the door of the courtroom, such as "authentication, hearsay, expert-reliability screening and statutory certification." The unresolved central question is not whether the evidence is admissible, but how much weight it is given to.¹ The data now comes into the courtroom easily, but seldom in the form of a question do courts ask about the science of the sensor that provides them with this data, creating a gap between admissibility and substantive reliability that the law of evidence has yet to close.

¹ Katherine E. Vinez, *The Admissibility of Data Collected from Wearable Devices*, 4 *Stetson J. Advoc. & L.* 1, 2 (2017).

Introduction

In December, 2015 in the early hours of morning investigators uncovered an unexpected witness that is a Fitbit which was strapped on the victim waistband. The device told a different story by recording footsteps for nearly an hour after her husband insisted that she had already been shot, which raised question that unexpectedly changed the direction of the investigation.² A routine fitness data point transformed into a important element of a homicide case. A single record of movement formed the foundation for the prosecutors to argue and almost 10years later the same evidence was examined again in an appeal before the Supreme Court of Connecticut. The debate case highlighted a larger transformation which reflected a growing trend in which wearable technology was increasingly recognised as an important source of forensic evidence in criminal proceedings and also valuable in civil litigation. The shift has occurred with almost no dedicated legislative attention. Wearable health data sits at the intersection of three bodies of law that were not designed with each other in mind: evidence law, which governs whether and how data reaches the trier of fact; data protection law, which governs whether the data may lawfully be collected, retained and disclosed in the first place; and consumer regulation, which governs whether the sensor generating the data is accurate enough to be trusted at all.³ This article examines how courts in the United States, Germany, Canada and India have handled wearable data offered as evidence and argues that the doctrinal seams between these three regimes rather than any single rule of evidence explaining why wearable data is simultaneously easy to admit and difficult to trust.

The Concept: Wearable Health Data as a Distinct Category of Digital Evidence

Wearable health data differs from ordinary digital evidence such as emails or call logs, in three structural respects. First, it is “continuously generated” rather than volitionally created i.e. a user does not “write” a heart-rate reading the way she writes a text message which complicates the hearsay and authorship analysis that traditionally governs documentary evidence. Second, it is “sensor-mediated”, the raw output is an electrical or optical signal that a proprietary algorithm converts into a step count, a sleep stage or a calorie estimate, so what is offered in evidence is not a fact but an inference generated by undisclosed code.⁴ Third, it is “cloud-

² State v. Dabate, 351 Conn. 428, 331 A.3d 1159 (2025).

³ Legal and Ethical Implications of Wearable Health Technologies: A Comparative Analysis of Privacy, Liability and Consent in India, EU and the United States, 5 Int'l J.L. Legal Rsch. (IJLLR), <https://www.ijllr.com/post/legal-andethical-implications-of-wearable-health-technologies-a-comparative-analysis-of-privacy-l>.

⁴ See Vinez, *supra* note 1.

mediated”, meaning the record a litigant obtains has typically passed through the manufacturer's servers, application programming interfaces and export tools before reaching a forensic examiner, layering custody and integrity questions onto the underlying reliability question.

These features place wearable data inarticulately between two founded evidentiary categories. It resembles a business record because it is generated systematically in the regular course of the device's operation yet it lacks the institutional accountability of a bank or hospital record because the entity maintaining the system is a consumer technology company with no duty of accuracy to the litigant. It resembles scientific or expert evidence because a jury cannot interpret a raw sensor log without explanation yet the underlying methodology is a trade secret rather than a peer-reviewed protocol. This hybrid character explains why courts have reached inconsistent conclusions about whether wearable data requires an expert-reliability hearing, a routine authentication showing or something in between.

Framework Features: The Statutory and Regulatory Architecture

A. U.S.A: Authentication, Hearsay and the Gatekeeping Function

In federal and most of the state courts, wearable data offered as evidence must clear two independent hurdles. ‘Authentication’ under “Federal Rule of Evidence 901” requires the defender to make a threshold showing that the record is what it purports to be, typically through testimony about the device, the export process and the chain of custody. “Amendments to Rule 902” have made certain machine-generated records self-authenticating where an accompanying certification establishes the reliability of the process that created them.⁵ Separately, where a party seeks to draw an inference from the data, for example, that a given heart-rate pattern is medically consistent with exertion, the defender must satisfy “Rule 702's reliability gatekeeping function” as articulated in “Daubert v. Merrell Dow Pharmaceuticals, Inc”., which asks whether the underlying methodology is testable, subject to peer review, and generally accepted.⁶ A number of states apply an equivalent standard derived from “Frye v. United States”. The “Porter hearing”, was the mechanism through which the trial court in Dabate admitted the victim's Fitbit data after finding it scientifically reliable, a finding the Supreme

⁵ Fed. R. Evid. 901, 902(13)–(14); see also Verifiable Provenance and Watermarking for Generative AI: An Evidentiary Framework for International Operational Law and Domestic Courts 4 (2026) (unpublished manuscript), <https://arxiv.org/abs/2605.21002>

⁶ Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 593–94 (1993); see also Vinez, *supra* note 1.

Court of Connecticut declined to disturb on appeal.⁷

Beyond the courtroom limit, no comprehensive federal statute governs the wearable itself. The “Health Insurance Portability and Accountability Act” applies only to “covered entities” and their business associates and consumer wearable manufacturers are, with narrow exceptions, outside that definition. The data such devices generate therefore falls into a regulatory gap even though it is at least as sensitive as clinical information.⁸ That regulatory vacuum matters for evidence law because it means the accuracy standards, calibration requirements and audit trails that might otherwise support a reliability finding simply do not exist as a matter of positive law; courts are left to construct reliability findings case by case on whatever technical evidence the parties choose to submit.

B. European Union: Data Protection as a Precondition to Admissibility

The “General Data Protection Regulation” directly does not regulate admissibility but it structures the lawfulness of the collection that precedes it. Wearable health metrics fall within the special category of “data concerning health” under “Article 9”, which may be processed only on narrow legal bases and unlawfully obtained data can be challenged on the footing that its use in litigation compounds the underlying violation.⁹ The European framework introduces two stage assessment absent from the American Federal Rules. Evidentiary value or authenticity of wearable data are evaluated by the courts to check whether the data is lawfully obtained or processed. This requirement is particularly relevant when such data is used for public interest purposes like Epidemiological studies or public health monitoring.¹⁰

C. India: Bharatiya Sakshya Adhiniyam and Sectoral Health data Statute

India presents the most evident gap between a mature electronic-evidence framework and an immature health-data framework. “Section 63 of the Bharatiya Sakshya Adhiniyam”, 2023, which replaced “Section 65B of the Indian Evidence Act, 1872”, governs the admissibility of

⁷ State v. Dabate, 351 Conn. 428, 331 A.3d 1159 (2025); see also State v. Porter, 241 Conn. 57, 698 A.2d 739 (1997).

⁸ Wearables: Where Do They Fall Within the Regulatory Landscape?, Int'l Ass'n of Privacy Pros. (IAPP) (2023), <https://iapp.org/news/a/wearables-where-do-they-fall-within-the-regulatory-landscape>; see also Is a HIPAA-Style De-Identification Standard Emerging in U.S. State Laws?, Int'l Ass'n of Privacy Pros. (IAPP) (Nov. 26, 2025), <https://iapp.org/news/a/is-a-hipaa-style-de-identification-standard-emerging-in-us-state-laws>.

⁹ Ethical and Legal Implications of Health Monitoring Wearable Devices: A Scoping Review, Soc. Sci. & Med. (2025).

¹⁰ Wearable Data: Can They Be Shared for a Public Interest, Such as Healthcare?, Joint Research Ctr., <https://jointresearch-centre.ec.europa.eu>.

any “computer output,” a term broad enough to capture data exported from a wearable's companion application.¹¹ Section 63(4) requires a certificate now, under the Act's Schedule, a dual certificate signed by both the person managing the device and a technical expert identifying the record describing how it was produced and confirming the integrity of the process without which the electronic record cannot be admitted regardless of its underlying relevance.¹² This certification requirement is, on its face, more demanding than the American authentication standard and it directly determines whether wearable data, for instance, step or heart-rate logs extracted from a smartwatch seized during investigation can be placed before an Indian court at all.

What India lacks is the sectoral regulation that would give that certificate substantive content. The “Digital Personal Data Protection Act, 2023”, treats health data as personal data without creating the heightened consent or security obligations that a “HIPAA or GDPR” style regime would impose and no notified rules yet specify calibration, retention or audit standards for consumer wearable manufacturers. The result is a procedurally rigorous but substantively hollow admissibility gate: an Indian court can be satisfied that a “Section 63” certificate is technically compliant while having no statutory benchmark against which to assess whether the sensor that generated the underlying reading was accurate in the first place, a gap that echoes the constitutional privacy architecture laid down in “K.S. Puttaswamy v. Union of India”, which recognised informational privacy as a facet of “Article 21” without itself supplying sector-specific data-accuracy standards.¹³

Judicial Interpretation

The earliest reported use of wearable data in adversarial proceedings was civil. In 2014, a Calgary personal-injury firm retained an analytics company to compare a client's post-accident Fitbit activity against population norms for her age and occupation, offering the comparison to quantify diminished capacity.¹⁴ The case never proceeded to a reasoned judgment on admissibility but it established the template still followed a decade later: wearable data used

¹¹ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63 (India).

¹² Bharatiya Sakshya Adhiniyam, No. 47 of 2023, sched. (India); Electronic Evidence Under BSA 2023: Section 63 Certificate Requirements & Supreme Court Interpretation, Bhatt & Joshi Assocs. (2026),

¹³ K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India); Digital Personal Data Protection Act, No. 22 of 2023, § 2(t) (India).

¹⁴ Parmy Olson, Fitbit Data Now Being Used in the Courtroom, Forbes (Nov. 16, 2014, 4:10 PM), <https://www.forbes.com/>; Samuel Gibbs, Court Sets Legal Precedent with Evidence from Fitbit Health Tracker, The Guardian (Nov. 18, 2014).

affirmatively, by the party who generated it, to corroborate a claim of physical harm.

Criminal courts have used the same data adversarially, against the wearer. In 2015, Pennsylvania investigators obtained a Fitbit Surge from a woman who reported a stranger rape; the device's step log showed her walking throughout the period she claimed to have been asleep and she was subsequently charged with filing a false report.¹⁵ The pattern recurred with greater consequence in “*State v. Dabate*”, where a Connecticut jury convicted a husband of murdering his wife after Fitbit data showed her moving for nearly an hour past the time he claimed an intruder had shot her; the trial court's admission of that data followed a “Porter” reliability hearing and the Connecticut Supreme Court affirmed both the conviction and the admissibility ruling on appeal in 2025, holding that the data was properly found scientifically reliable notwithstanding the defence's challenge to Fitbit's accuracy.¹⁶ A comparable evidentiary role was played by smartphone-based health data rather than a dedicated wearable in the 2018 Freiburg murder trial in Germany, where investigators used the defendant's Apple Health application, which recorded two spikes of activity classified as “climbing stairs,” to corroborate a theory that he had dragged and disposed of his victim's body during a period otherwise unaccounted for by surveillance footage.¹⁷ German investigators there took the unusual step of having an officer of similar build re-enact the suspected movements while wearing an iPhone, generating a comparison dataset to test whether the “climbing stairs” classification was consistent with the alternative, incriminating explanation, an ad hoc, court-adjacent validation exercise that substituted for any formal reliability standard.

India has not yet produced a reported decision addressing wearable device data specifically but its jurisprudence on electronic evidence more broadly supplies the interpretive framework that will govern such cases when they arise. The Supreme Court's decision in “*Anvar P.V. v. P.K. Basheer*” held that a certificate under Section 65B, was a mandatory condition precedent to the admissibility of secondary electronic evidence, overruling an earlier, more permissive approach that had treated the certificate as merely directory.¹⁸ The Court revisited and clarified that holding in “*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*”, confirming that

¹⁵ Fitness Trackers Add to Flood of Digital Evidence in Courts, Ind. Law. (Aug. 10, 2016).

¹⁶ *State v. Dabate*, 351 Conn. 428, 331 A.3d 1159 (2025).

¹⁷ Apple Health App 'Used as Evidence in Murder Trial', Digital Health (Jan. 16, 2018), <https://www.digitalhealth.net/2018/01/apple-health-data-murder-trial/>; German Police Use Health App Data as Evidence in Murder Case, Privacy Int'l, <https://privacyinternational.org/examples/1953/german-police-use-healthapp-data-evidence-murder-case>.

¹⁸ *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India), overruling in part *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 S.C.C. 600 (India).

the certificate requirement is mandatory but that a court may, in appropriate circumstances, permit the certificate to be produced at a later stage of proceedings rather than treating its absence as fatal in every case.¹⁹ Because “Section 63 of the Bharatiya Sakshya Adhiniyam” substantially re-enacts this framework, commentators expect the “Anvar-Arjun Panditrao” line of authority to govern the admissibility of wearable-derived records extracted during investigation with the new dual-signature certificate adding a further, untested layer of technical compliance.²⁰

Practical Implications

The doctrinal position outlined above has three important considerations for the litigators. The first concerns the need to preserve and unbroken chain of custody as wearable data is generally transmitted through the manufacturer’s cloud systems before forensic examinations, any break in that chain such as undocumented export, mismatch of hash values, a post firmware update may undermine confidence in the evidence and question the evidence’s reliability.²¹ Second, expert testimony is increasingly indispensable rather than optional because the algorithm converting raw sensor signals into a usable metric is proprietary, only a witness with access to or specialised knowledge of, that conversion process can meaningfully explain or challenge as to what the exported number actually represents, a burden that favours resource-rich litigants and prosecuting authorities over individual defendants and claimants. Third, discovery practice has had to adapt: “the 2015 amendment to Rule 26 of the Federal Rules of Civil Procedure”, which requires discovery to be proportional to the needs of the case is now regularly invoked to resist broad requests for a party’s complete wearable data history confining discovery to the period genuinely in issue.²²

In India, the practical burden falls differently because Section 63 makes the certificate a condition precedent rather than a mere formality, investigating agencies and private litigants alike must build compliance into the acquisition process from the outset, since courts have shown limited tolerance for curing a defective or absent certificate after the fact, notwithstanding the procedural flexibility recognised in “Arjun Panditrao case”. Practitioners advising clients on wearable-derived evidence in India should therefore treat the dual-signature

¹⁹ Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India).

²⁰ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, supra note 11.

²¹ Why Proper Digital Forensics Is Critical for Admissibility, Team Avalon (2026).

²² Fitness Trackers Add to Flood of Digital Evidence in Courts, supra note 15.

certificate not as paperwork but as substantive proof, obtained contemporaneously with acquisition wherever feasible.

Contemporary Issues

Three developments complicate the picture further. First, security incidents at wearable manufacturers have demonstrated that the same infrastructure relied upon to authenticate data in litigation is also a target for compromise. In 2026, the Bengaluru-based wearable company “Ultrahuman” disclosed that attackers had used credentials stolen from an employee's malware infected laptop to gain read-only access to an internal analytics system, exposing wellness and account data for a subset of its users; the company took more than two months to notify affected individuals.²³ Such incidents matter for evidence law because they undermine the very premise that manufacturer-held records are trustworthy repositories on which authentication under provisions like “Federal Rule of Evidence 901” and “Section 63 of the Bharatiya Sakshya Adhiniyam” ultimately rests. A party seeking to rely on wearable data can now be met with a plausible objection that the record's integrity cannot be assumed absent proof that the relevant systems were uncompromised at the time in question.

Second, the regulatory gap identified has widened rather than narrowed. Scholarship surveying manufacturer privacy policies across leading wearable brands has found that consent mechanisms remain lengthy, opaque and poorly understood by users, while data continues to move to advertising and analytics partners outside any health-specific oversight regime.²⁴ This matters evidentially because data obtained without meaningful consent, and later sought to be used against the individual who generated it, raises fairness objections distinct from but layered on top of ordinary admissibility analysis, particularly in jurisdictions such as India where constitutional privacy protection under “Puttaswamy” has not yet been operationalised through sector-specific health-data rules.

Third, the devices themselves are becoming more, not less, forensically ambitious. Contemporary wearables increasingly pair with computer-vision systems and generate continuous physiological streams intended for behavioural and health research, a convergence that will make the volume and inferential richness of wearable evidence available to courts

²³ Ultrahuman Suffers a Major Security Breach, Exposing Users' Wellness Data: How Did It Happen?, MediaNama (2026).

²⁴ Privacy in Consumer Wearable Technologies: A Living Systematic Analysis of Data Policies Across Leading Manufacturers, PMC (2026).

substantially greater within the next several years.²⁵ Without a corresponding development of accuracy standards, certification protocols, or sector-specific privacy legislation, courts will be asked to evaluate increasingly sophisticated inferential claims using an evidentiary toolkit designed for a much simpler generation of devices.

Conclusion and Recommendations

Within a decade, wearable health data has moved from evidentiary curiosity to a recurring feature of civil and criminal litigation across multiple jurisdictions. What has not moved at a comparable pace is the legal infrastructure surrounding it. The United States relies on authentication and expert-reliability doctrines developed for other technologies; the European Union filters admissibility through a data-protection lens that was not designed with courtroom use in mind; and India possesses a rigorous certification regime for electronic evidence in general but no sectoral health-data statute to give that regime substantive content when the record at issue is a heart-rate log rather than an email.

Three reforms would narrow this gap. First, evidentiary rules in all three jurisdictions should require, as a condition of admitting wearable data for a substantive inferential purpose, disclosure of the manufacturer's validation methodology or independent accuracy studies, rather than treating a bare certificate of authenticity as sufficient. Second, sectoral health-data legislation whether an amendment to HIPAA's covered-entity definition in the United States or the framing of rules under the "Digital Personal Data Protection Act" in India should establish minimum security and accuracy obligations for wearable manufacturers, both to protect users and to give courts a benchmark against which to assess reliability. Third, forensic and legal training institutions should develop standard protocols for the acquisition and certification of wearable data, comparable to those that now exist for mobile phone extraction, so that the dual-signature certificate under "Section 63 of the Bharatiya Sakshya Adhiniyam" and its analogues elsewhere are backed by genuine technical competence rather than procedural formality. Until such reforms occur, wearable health data will remain what Dabate and the Freiburg trial together illustrate: evidence that courts are increasingly willing to admit but that the law has not yet fully learned how to test.

²⁵ Wearable and Computer Vision Data for Health and Behaviour Research, *Nature* (Aug. 8, 2025).

References

- https://aphc.gov.in/docs/imp_judgements/Anvar%20PV%20case.pdf
- https://aphc.gov.in/docs/imp_judgements/Arjun%20Panditrao%20Khotkar%20_%20Kailash%20Kushanrao%20Gorantyal%20And%20Ors._1701334263.pdf
- <https://www.drishtijudiciary.com/to-the-point/bharatiya-sakshya-adhiniyam-&-indian-evidence-act>
- <https://bhattandjoshiassociates.com/electronic-evidence-under-bsa-2023section-63-certificate-requirements-supreme-court-interpretation/>
- <https://supreme.justia.com/cases/federal/us/509/579/>

Case laws

- Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India)
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
- Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579 (1993).
- K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India)
- State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 (India).
- State v. Dabate, 351 Conn. 428, 331 A.3d 1159 (2025).
- State v. Porter, 241 Conn. 57, 698 A.2d 739 (1997).