LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Growing Role Of Wearable Health Tech In Criminal Probes

By **Pei Pei Cheng de Castro and Jennifer Hopkins** (March 21, 2025, 4:58 PM EDT)


Pei Pei Cheng de Castro


Jennifer Hopkins

Wearable health devices have become a fashion, fitness and wellness necessity in modern society, seamlessly integrating into our daily routines.

Smart health technologies are embedded in our smart devices, including Apple Watches, Fitbits, Whoop wearable technology and the increasingly popular smart rings.

These wearable devices collect a wide range of personal health data, such as heart rates, step counts, walking speed, blood oxygen levels, sleep patterns and stress levels.[1] With a few clicks of a button, individuals can access and share this data with health care professionals and their social circles.

This underscores a deeper issue: our increasing reliance on wearables to track, monitor and analyze intimate health data. This growing dependence raises significant concerns about privacy, security and the potential for misuse of such data, especially in criminal investigations.

While all this data can arguably help improve our health and motivate positive changes, the data contained in these devices could also potentially serve as key evidence against targets of criminal investigations and criminal defendants. The use of such data in investigations also presents significant constitutional and reliability concerns.

Is this data reliable enough to be used in criminal proceedings? Do proven correlations between certain health metrics and specific criminal behavior need to exist?

For example, could a significant spike in heart rate recorded on a device be used to suggest that a defendant was involved in a violent act, such as a murder? Are there concerns under the Fourth Amendment, which protects against unreasonable searches and seizures, and the Fifth Amendment right to remain silent?

This article explores these questions, and provides pointers for defense counsel in cases involving health-tracking device data.

Cases Involving Wearable Health Data

Several high-profile cases illustrate the complexities and challenges surrounding the use of wearable

health data in criminal investigations and prosecutions.

One example is the case of Anthony Aiello, a 90-year-old man accused of murdering his stepdaughter, Karen Navarra, in her home in San Jose, California.[2] Investigators relied heavily on data from Navarra's Fitbit to establish a timeline of her final moments on Sept. 8, 2018.[3]

According to the Fitbit, there was a spike in her heart rate at approximately 3:20 p.m., followed by a rapid decline in her heart rate, which stopped at 3:28 p.m. — just before Aiello left the house.[4] This data, paired with other evidence such as video footage and bloodstained clothing found at Aiello's residence, helped to tie Aiello to the crime.[5]

However, the Superior Court of California case was dismissed after Aiello's 2019 death in custody, leaving unresolved questions about the accuracy and reliability of wearable health data in criminal cases.[6]

Another case that attracted significant attention was the 2022 conviction of Richard Dabate, who was found guilty of murdering his wife, Connie, in December 2015.[7] Dabate claimed that an intruder shot his wife while he was bound to a chair in their basement, but data from Connie's Fitbit contradicted his version of events.[8]

The Fitbit data showed that she was home for at least 48 minutes after returning from the YMCA, walking at a normal pace and engaging in other activities such as posting on Facebook and messaging a friend.[9] This evidence directly undermined Dabate's claim that she was killed immediately upon arriving home.

The Dabate case is now under further scrutiny with the Connecticut Supreme Court.[10] At the core of his appeal, Dabate contended that the Fitbit data is scientifically unreliable and cannot be accurately measured.[11]

He argued that the expert witness, Dr. Keith Diaz, a behavioral medicine expert who testified before the Tolland Judicial District Superior Court about the Fitbit data, could not explain how the device works or the methodology behind it.[12]

In response, the prosecution restated the testimony of Diaz.[13] Diaz explained that the Fitbit uses an "accelerometer," in order to "measure movement on three planes," converting that data into step counts using a "proprietary algorithm"; thus demonstrating his understanding of the device's functionality and underlying methodology, directly contradicting the defense's claim that he was unable to explain how it works.[14]

He testified that the particular Fitbit model that Connie wore had been tested extensively and was found to be 98% accurate in terms of step counts when worn on the hip.[15] Diaz also pointed out that the Fitbit has been validated in numerous peer-reviewed studies and is widely accepted in the scientific community for clinical use.[16]

While Dabate's defense argued that the Fitbit's proprietary algorithm makes the data unreliable, the prosecution countered that Diaz's testimony supports its general acceptance and accuracy in step counting.

The prosecution, on appeal, asserted that the trial court acted within its discretion in admitting the Fitbit

records, highlighting that the expert testimony demonstrated the data's accuracy and general acceptance in the scientific community.[17] On Oct. 20, 2024, the Connecticut Supreme Court heard oral arguments, and a decision is still pending.[18]

In another significant case, State v. Burch, the Wisconsin Supreme Court determined that expert testimony was not required, as the underlying Fitbit data was widely used and self-authenticating, and upheld the conviction of George Burch.[19]

Burch was convicted of the murder of Nicole VanderHeyden, with evidence including data from the Fitbit belonging to VanderHeyden's boyfriend, Douglass Detrie.[20] The Fitbit data showed that Detrie had been inactive during the time of the murder, directly contradicting Burch's defense that Detrie was involved in the crime.[21]

Along with this, GPS data from Burch's phone placed him at key locations near the crime scene, helping to solidify the case against him.[22] Burch was sentenced to life in prison without the possibility of parole in 2018.[23]

He appealed his conviction to the Wisconsin Supreme Court, arguing that the Fitbit evidence should have been excluded because expert testimony was required to establish the reliability of the data and that the data was insufficiently authenticated.[24] However, the Supreme Court upheld the conviction and found that expert testimony was not required, as the Fitbit data was not considered unusually complex or esoteric.[25]

The court reasoned that the technology behind step-counting devices like the Fitbit is widely understood by the general public, given their common use in consumer products such as smartphones and fitness trackers.[26] Since jurors could reasonably understand the basic function of the device and its reliability, expert testimony was deemed unnecessary.

The court also held that the Fitbit records were sufficiently authenticated, as they were accompanied by an affidavit from a custodian of Fitbit's records, confirming their accuracy and authenticity.[27] The court concluded that once the records were authenticated, it was up to the court below, as the fact-finder, to assess the weight and credibility of the evidence.[28]

In another case, Terrence Chip Ogle of Yakima, Washington, was convicted last year of murdering his girlfriend's toddler, Alexander Lynch, in 2020.[29] The prosecution used heart-rate data from the Apple Watch worn by Ogle's girlfriend, Marie Kotler, to demonstrate that Kotler was asleep at the time her son was likely injured, further supporting the case against Ogle.[30]

The watch data showed that Kotler's heart rate remained steadily between 52 and 71 beats per minute from 1 a.m. to 2 a.m., with a spike occurring after she woke up to attempt CPR.[31]

Despite challenges from Ogle's defense regarding the authenticity of the data, the Yakima County Superior Court accepted it as evidence, ultimately contributing to his conviction for second-degree murder in the death of the 15-month-old.[32] Ogle has filed an appeal.

Finally, in a case from last year, Laken Riley's Garmin smartwatch provided key evidence in the investigation of her Feb. 22, 2024, murder in Athens, Georgia.[33] The smartwatch data showed a significant disruption in her heart rate around 9:10 a.m., coinciding with her activation of the SOS function on her phone and a 911 call.[34]

The smartwatch also tracked her movement as she was dragged into the woods, eventually showing no further movement after 9:28 a.m., marking the likely time of her death.[35] This crucial data, along with DNA evidence, played a major role in identifying José Ibarra as the perpetrator.[36]

During the trial in Athens-Clarke County Superior Court, Ibarra's attorney argued that the evidence was circumstantial, but in November, Ibarra was convicted of murder and sentenced to life in prison.[37] Ibarra has filed a motion for a new trial.

HIPAA Concerns

The use of wearable health data in criminal investigations introduces significant legal challenges, particularly regarding privacy and data protection. A key issue is the potential applicability of the Health Insurance Portability and Accountability Act, or HIPAA., which governs the protection of health information.[38]

HIPAA was designed to protect individuals' health data, especially in the context of healthcare providers, insurance companies, and other entities involved in medical treatment.

However, the ambiguity surrounding whether data from wearable devices is protected under HIPAA is a significant challenge. Wearable devices like the Fitbit, Apple Watch or Whoop collect extensive personal health data, but much of this data is not transmitted through healthcare providers or covered entities.

HIPAA protections apply primarily to healthcare providers, insurers, and certain other entities that handle medical records or health data in a clinical context. Therefore, health data generated by consumer-grade wearables — particularly when shared with third parties or in a criminal investigation — may fall outside the scope of HIPAA protections.

For example, if a Fitbit user voluntarily shares their data with a law enforcement agency, this data could be used in a criminal investigation, but it would not necessarily be protected by HIPAA, since it is not being shared with a healthcare provider.

This creates a potential gap in privacy protections. On the other hand, if the data is shared with a healthcare provider, it is considered protected health information under HIPAA, and would require a subpoena.

The lack of clear guidelines on the scope of HIPAA in relation to wearable health devices means that law enforcement agencies may have greater access to personal health data than individuals expect. This could lead to significant privacy concerns, especially if the data is used without the individual's consent or if it is shared with third parties who are not bound by HIPAA confidentiality requirements.

Constitutional Concerns

The use of wearable health data also raises significant constitutional concerns, particularly in relation to the Fourth and Fifth Amendments. The Fourth Amendment protects against unreasonable searches and seizures, meaning law enforcement generally needs a warrant to access personal data. But wearable devices present unique challenges.

Courts have yet to definitively determine whether data accessed from a defendant's wearable device

requires a warrant, especially if the data has been voluntarily shared by the defendant or a third party.

The issue becomes even more complex when the data could be used to incriminate the defendant. Do prosecutors have to identify in the warrant that they are going to review personal health data on the device as well?

The Fifth Amendment protects against self-incrimination, and questions arise about whether a defendant could be compelled to unlock or provide access to their wearable device.

Similar to cases involving smartphones,[39] courts may eventually address whether accessing personal health data from devices like the Apple Watch or Fitbit violates the defendant's right to remain silent. If the data obtained is used to suggest the defendant's involvement in a crime, it raises concerns about whether forcing the defendant to provide access to their wearable device would violate their constitutional rights.

Possible Defense Arguments

In cases where wearable health data is used against a defendant, particularly if the data appears to provide incriminating evidence, defense attorneys should continue to raise reliability arguments. These arguments could include questioning the device's data collection and analysis methods and algorithms, as well as its validation process, which may not always be accurate or foolproof.

Defense attorneys should also scrutinize potential user input errors, inconsistencies in sensor technology, and variations in sensor quality that could lead to misleading data.[40] Additionally, they should examine the individual's use of the device — such as how it was placed or worn during data collection — as improper placement can significantly affect the reliability of the readings.[41]

Defense counsel should question the direct correlation between aberrant data and criminal behavior, as many factors unrelated to criminal activity — such as physical exertion, stress, or pre-existing conditions — could cause similar irregularities. Finally, should the government be required to obtain its witnesses' data, which can be exculpatory or used to challenge the assessment of the surrounding data?

Additionally, if data from a wearable device is obtained without a warrant or through unclear consent, defense attorneys could invoke Fourth Amendment protections, arguing that the data was illegally seized or that the defendant's consent was not knowingly and voluntarily given.

If the data is only personally held by the wearer of the device or kept behind a passcode, attorneys could invoke the Fifth Amendment arguing that compelling its disclosure forces the defendant to affirm its existence, accuracy and control, making the act of production testimonial. If law enforcement accessed the data without proper safeguards or authorization, the evidence could be challenged as inadmissible.

Conclusion

As wearable health devices increasingly become integrated into criminal investigations, legal systems must evolve to address the growing concerns surrounding privacy, data accuracy and constitutional protections.

Given the prevalence of these devices, there is an urgent need for clearer guidelines about how this data is accessed, used and protected in the context of criminal investigations. As technology advances, it is

essential to balance law enforcement's need for evidence with the individual's fundamental rights to privacy and self-incrimination.

This issue is not just about technicalities; it strikes at the core of personal freedoms and the constitutional safeguards designed to protect them.

Just as wearables track our every move, the legal system must tread carefully — ensuring that, in the pursuit of justice, it doesn't take steps that infringe on the very rights it seeks to uphold.

Pei Pei Cheng de Castro is a partner and Jennifer Hopkins is an associate at Barclay Damon LLP.

[1] See, e.g., 7 ways wearable technology can help you reach your health goals, UCLA Health (Feb. 4, 2025), https://www.uclahealth.org/news/article/7-ways-wearable-technology-can-help-you-reach-your-health.

[2] See Hannah Fontaine, The Rise of Smartwatch Data in Criminal Cases, Harv. Undergraduate L. Review (Spring 2020), https://hulr.org/law-in-the-news/the-rise-of-smartwatch-data-in-criminal-cases.

[3] See Christine Hauser, Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing, N.Y. Times (Oct. 3, 2018), https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html.

[4] See id.

[5] See id.

[6] See Elderly Suspect In San Jose Fitbit Murder Dies In Custody, CBS San Francisco (Sept. 11, 2019), https://www.cbsnews.com/sanfrancisco/news/elderly-suspect-san-jose-fitbit-murder-dies-custody/.

[7] See Amanda Pitts, Ellington man's conviction over wife's murder appealed to CT Supreme Court, NBC Connecticut (Oct. 30, 2024), https://www.nbcconnecticut.com/news/local/ellington-mans-conviction-over-wifes-murder-appealed/3422148/.

[8] See Christine Hauser, In Connecticut Murder Case, a Fitbit Is a Silent Witness, N.Y. Times (Apr. 27, 2017), https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html.

[9] See Brief of the State of Connecticut-Appellee, State of Connecticut v. Richard Dabate, S.C. 20749, at 17-18 (filed June 11, 2024).

[10] See Pitts, supra note 7; see also Supreme and Appellate Court Case Detail, State of Connecticut v. Richard G.
Dabate, https://appellateinquiry.jud.ct.gov/CaseDetail.aspx?CRN=77767&Type=AppealNo (last visited Feb. 6, 2025).

[11] See Brief of the Defendant-Appellant, State of Connecticut v. Richard Dabate, S.C. 20749 (filed Sept. 6, 2023).

[12] See id.

[13] See Brief of the State of Connecticut-Appellee, supra note 9, at 53-54.

[14] Id. at 53.

[15] See id.

[16] See id. at 53-54.

[17] See id. at 55-56.

[18] See Supreme and Appellate Court Case Detail, State of Connecticut v. Richard G. Dabate, supra note 10.

[19] See State v. Burch, 2021 WI 68, 398 Wis. 2d 1, 961 N.W.2d 314.

[20] See Lilly Dancyger, Fitbits Are Snitching on Criminals — Here's How, Rolling Stone (Oct. 4, 2018), https://www.rollingstone.com/culture/culture-news/fitbit-apple-watch-crime-help-solve-733050/.

[21] See Burch, 2021 WI 68, ¶ 4.

[22] See id.

[23] See Paul Srubas, George Burch gets life in prison without parole for murder of Nicole VanderHeyden, Green Bay Press-Gazette (May 4, 2018), https://www.greenbaypressgazette.com/story/news/2018/05/04/burch-sentenced-life-prison-parole-nicole-vanderheyden-murder/561154002/.

[24] See Burch, 2021 WI 68, ¶ 27.

[25] See id. at ¶ 31.

[26] See id.

[27] See id. at ¶ 34.

[28] See id.

[29] See Donald W. Meyers, Terrence Chip Ogle found guilty in 2020 killing of West Valley toddler; juror says medical testimony was key, Yakima Herald-Republic (Aug. 25, 2024), https://www.yakimaherald.com/news/ local/crime_and_courts/terrence-chip-ogle-found-guilty-in-2020-killing-of-west-valley-toddler-juror-says-medical/article_b7b0bd36-625a-11ef-bec7-174d1bbcfefd.html.

[30] See Donald W. Meyers, Court OKs use of Apple Watch data in trial of man accused in West Valley toddler's death, Yakima Herald-Republic (Aug. 21, 2024), https://www.yakimaherald.com/news/local/crime_ and_courts /court-oks-use-of-apple-watch-data-in-trial-of-man-accused-in-west-valley/article_e8b60cda-5f33-11ef-b77d-3f883242265f.html.

[31] See id.

[32] See Donald W. Meyers, Terrence Ogle sentenced to 28 years for killing his girlfriend's toddler son, Yakima Herald-Republic (Nov. 15, 2024), https://www.yakimaherald.com/news/local/crime_and_courts/terrence-ogle-sentenced-to-28-years-for-killing-his-girlfriends-toddler-son/article_ed05d78c-a2ba-11ef-93bb-cbdad1d35ac7.html.

[33] See Ashley R. Williams et al., How smartwatch left clues in killing of Laken Riley, prosecutors say, ABC 30 (Nov. 16, 2024), https://abc30.com/post/laken-riley-case-jose-ibarra-trial-prosecutors-share-how-911-call-smartwatch-left-clues-augusta-university-students-death/15550893/.

[34] See Ashley R. Williams, Laken Riley went for a morning jog. Less than 30 minutes later, she was dead. What we know about her final moments, CNN (Nov. 17, 2024), https://www.cnn.com/2024/11/17/us/laken-riley-killing-final-moments-timeline/index.html.

[35] See id.

[36] See id.

[37] See Kate Brumback, Man convicted of killing Laken Riley sentenced to life in prison without parole, AP News (Nov. 20, 2024), https://apnews.com/article/georgia-nursing-student-laken-riley-immigrant-d8d75ccc6d81e7a88eb7890829d9fc9c.

[38] See Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936; see also HIPAA Privacy Rule, 45 C.F.R. §§ 160, 164 subpart A, E.

[39] We previously discussed how courts have addressed the constitutional challenges of compelling defendants to unlock electronic devices, whether through passcodes, fingerprints, or other biometric methods, in a related article on this topic. See Pei Pei Cheng de Castro & Jennifer Hopkins, Must Defendants Unlock Their Cellphones? What The Law Says, CityLand NYC (Nov. 25, 2024), https://www.citylandnyc.org/must-defendants-unlock-their-cellphones-what-the-law-says/.

[40] See Alaa Khushhal et al., Validity and Reliability of the Apple Watch for Measuring Heart Rate During Exercise, Sports Med Int. Open (Oct. 2017), https://pmc.ncbi.nlm.nih.gov/articles/PMC6226089/#sec12 ("[T]he validity of measuring HR decreases with increasing exercise intensity.").

[41] See Lauren Lederer, Considerations while using Fitbit Data in the All of Us Research Program, All of Us (Feb. 2023), https://support.researchallofus.org/hc/en-us/articles/9651723386388-Considerations-while-using-Fitbit-Data-in-the-All-of-Us-Research-Program ("[I]mproper Fitbit wear can also become a source of error. Because wrist-based devices such as Fitbits can often misclassify arm movements that occur when the entire body is not moving, they can underestimate or overestimate activity.").