npj | digital medicine

Article

Published in partnership with Seoul National University Bundang Hospital

https://doi.org/10.1038/s41746-025-01757-1

Privacy in consumer wearable technologies: a living systematic analysis of data policies across leading manufacturers

Check for updates

Cailbhe Doherty[1,2] ✉, Maximus Baldwin[2,3], Rory Lambe[1,2], Marco Altini[4] & Brian Caulfield[1,2]

The widespread adoption of consumer wearable devices has enabled continuous biometric data collection at an unprecedented scale, raising important questions about data privacy, security, and user rights. In this study, we systematically evaluated the privacy policies of 17 leading wearable technology manufacturers using a novel rubric comprising 24 criteria across seven dimensions: transparency, data collection purposes, data minimization, user control and rights, third-party data sharing, data security, and breach notification. High Risk ratings were most frequent for transparency reporting (76%) and vulnerability disclosure (65%), while Low Risk ratings were common for identity policy (94%) and data access (71%). Xiaomi, Wyze, and Huawei had the highest cumulative risk scores, whereas Google, Apple, and Polar ranked lowest. Our findings highlight inconsistencies in data governance across the industry and underscore the need for stronger, sector-specific privacy standards. This living review will track ongoing policy changes and promote accountability in this rapidly evolving domain.

The global adoption of wearable devices has transitioned rapidly from niche applications to widespread consumer use. In 2024, worldwide shipments of wearables—including smartwatches, fitness trackers, and hearables—surpassed 543 million units, reflecting a 6.1% increase from the previous year[1]. By 2029, smartwatch users alone are projected to reach 740 million globally[1].

This growth is largely driven by advancements in sensor technology, enabling wearables to continuously monitor a wide range of physiological and behavioural metrics at lower price points and smaller form factors[2,3]. Modern devices can monitor a variety of health parameters such as heart rate, cardiorespiratory fitness, sleep patterns, and physical activity levels[2,4] – albeit with variable accuracy[4]. For example, a typical smartwatch can record second-by-second data on steps and heart rate, generating tens of thousands of individual data points per day[5,6]. With more than 500 million wearables in use globally[1], the total data footprint of this ecosystem reaches into the trillions of data points annually.

The capacity of consumer wearables to continuously monitor a range of health metrics can facilitate users to make real-time adjustments to their behaviours, leading to increased physical activity[7,8], better sleep hygiene[9,10], and enhanced athletic performance[11,12]. At a societal level, this aggregated data holds promise for public health initiatives, providing insights into physical activity trends[13,14], disease risks[15,16], the early detection of pandemics [17–19] and the health effects associated with climate change[20,21]. With recent advances in artificial intelligence and machine learning[22], the value of wearable derived biodata will continue to evolve, unlocking new possibilities to personalise health interventions, advance scientific research, optimise healthcare delivery, and inform public policy[23,24].

However, the proliferation of biometric data collection through wearables also introduces significant risks to individuals and society. These include cybersecurity breaches, data misuse, consent violations, discrimination against vulnerable populations, biometric persecution, and widespread surveillance[25,26]. For instance, insurers might use health data to risk-profile individuals, potentially leading to higher premiums[27]. Employers could access data reflecting negatively on candidates' health or productivity, influencing hiring decisions[28]. Additionally, health biodata is a highly valued commodity on the Dark Web. According to a 2021 Trustwave report, healthcare data records are worth up to $250 per record, compared to $5.40 for a payment card, due to the comprehensive personal information they contain[29,30].

[1]School of Public Health, Physiotherapy and Sports Science, University College Dublin, Dublin, Ireland. [2]Insight Research Ireland Centre for Data Analytics, University College Dublin, Dublin, Ireland. [3]Institute for Sport and Health, University College Dublin, Dublin, Ireland. [4]Department of Human Movement Sciences, Vrije Universiteit Amsterdam, Amsterdam, Netherlands. ✉e-mail: cailbhe.doherty@ucd.ie

Despite regulatory frameworks designed to protect consumers, the commercial ecosystem surrounding wearable devices continues to pose substantial privacy risks. Many companies are incentivised to gather and monetise extensive amounts of user data[31], often concealing the scope of these practices behind dense, difficult-to-read privacy policies[32,33]. Recent data breaches underscore these vulnerabilities: a security incident exposed over 61 million fitness tracker records[34], and a breach involving UnitedHealth compromised the health information of 100 million individuals[35]. These incidents highlight the ongoing challenges and ethical dilemmas in managing wearable data responsibly.

In response, various governmental regulations set baseline protections for consumer data. Frameworks such as the European Union's General Data Protection Regulation (GDPR)[36], the United States' Health Insurance Portability and Accountability Act (HIPAA)[37], the California Consumer Privacy Act (CCPA)[38], Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)[39], and the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules[40] form a global patchwork of protections aimed at balancing privacy with innovation and interoperability. However, regional disparities and opaque third-party data practices create regulatory grey areas that some companies exploit, often prioritising operational flexibility over user privacy[41,42].

In this landscape, consumers bear much of the responsibility to protect their own privacy. Yet, privacy fatigue—a condition where consumers are overwhelmed by frequent, lengthy privacy disclosures—leaves many disengaged. Research shows that up to 97% of users accept terms and conditions without fully understanding them[32,42,43]. To support consumers, independent initiatives such as Mozilla's Privacy Not Included[44], Consumer Reports' Digital Standard[45], and NOYB.eu[46] aim to hold companies to higher privacy standards, offering accessible evaluations that encourage ethical data practices. However, these efforts, along with current regulations, lack specific standards for the consumer wearables industry. To date, no systematic evaluation of wearable device privacy policies has been conducted, leaving a significant gap in protections for this rapidly expanding sector.

This research seeks to fill this gap by systematically evaluating the privacy policies of consumer wearable devices. The primary aim is to develop an evaluation framework tailored to this product class, synthesising existing regulatory standards, legislative guidelines, and best practices from consumer advocacy organisations. The secondary objective is to apply this framework to critically evaluate the privacy policies of major wearable manufacturers. Through this dual approach, the study aims to identify deficiencies in current practices, highlight risks to consumer rights, and provide actionable recommendations for improving privacy policies.

Results

We collated the privacy policies from 17 different wearable device manufacturers to evaluate privacy risk across the seven dimensions and 24 criteria of the evaluation framework. Most companies published a single global policy, often with jurisdiction-specific addenda (e.g., for EU, California, or Canada). In such instances, we evaluated the global policy only. The privacy policies evaluated varied widely in length, with an average of 6113 words (SD = 2300). The longest policy, at 12,125 words (WHOOP), while the shortest was 4408 (Apple).

Across the 17 manufacturers included in this review, the most recently available privacy policy updates ranged from May 2023 to April 2025. Based on observed version histories, policy update frequency varied substantially across companies. Garmin, Withings, and Google provide accessible archives or version logs, with Garmin publishing six updates between 2020 and 2025 and Withings publishing 12 since 2017. In contrast, companies such as Coros did not publish explicit version histories or last-modified timestamps. From available records, a typical policy revision cycle appears to occur approximately once every 9–15 months, though some firms (e.g., Garmin and Withings) revise more frequently, and others rarely update publicly visible documentation. A full version log is available in our publicly archived repository (https://osf.io/vtwne/?view_only=1da176f8d0dc4574a454add4a4759c50).

Inter-rater reliability analysis

The overall inter-rater agreement for the evaluation was 89.3% (Cohen's Kappa = 0.893, 95% CI = [0.855–0.931]), indicating excellent agreement. Dimension-specific inter-rater reliability ranged from 0.469 to 1. The highest agreement was observed for criterion #6 (data collection), criterion #12 (data retention), criterion #13 (data control), and criterion #22 (security over time), with Cohen's Kappa = 1 for all these criteria. The lowest agreement was observed for the criterion related to identity policy (Cohen's Kappa = 0.469).

Overall risk

The evaluation revealed significant variability in privacy and data security practices across wearable device companies, with certain criteria demonstrating a high prevalence of risks.

High Risk ratings were most frequently observed for criteria related to Transparency Reporting (criterion #2, 76% High Risk), Vulnerability Disclosure Programs (criterion #23, 65% High Risk), and Breach Notification (criterion #24, 59% High Risk). Specifically, a large proportion of companies failed to provide clear and comprehensive transparency reports regarding data sharing with governments or third parties, including legal justifications and affected accounts. Similarly, most companies lacked formalised vulnerability disclosure programs and robust breach notification processes, posing significant risks to data security and incident response.

Criteria associated with data control and user autonomy also raised concerns. Specifically, Privacy by Default settings (criterion #8, 41% High Risk), Threat Notification (criterion #3, 53% High Risk), User Notification about Third-Party Requests (criterion #1, 47% High Risk) and Minimal Data Collection (criterion #7, 24% High Risk) were often poorly implemented, indicating that companies frequently collect unnecessary data and fail to adopt privacy-protective defaults. Furthermore, only a minority of companies achieved optimal scores for Data Deletion (criterion #16, 24% High Risk), where clear deletion policies and practices were often inadequate.

Conversely, Low Risk ratings were predominantly observed for Identity Policy (criterion #4, 94% Low Risk), Data Access (criterion #15, 71% Low Risk), and Control Over Targeted Advertising (criterion #14, 65% Low Risk). This suggests that most companies allow users to access their data in structured formats, disable targeted advertising, and register accounts without requiring government-issued identification. Additionally, criteria like Data Collection (criterion #6, 71% Low Risk) and Purpose Limitation (criterion #10, 53% Low Risk) reflect a general adherence to the principle of data transparency and purpose-specific data collection.

The full results of the evaluation, stratified by company according to each dimension of the evaluation framework, and the specific criteria that made up each dimension, are displayed in Table 1.

Company and criterion risk

The companies with the highest number of 'high risk' ratings were Xiaomi (16), Wyze (15) and Huawei (14). Conversely, the companies with the lowest number of 'high risk' ratings were Apple (2), Fitbit (2), Google (2), Oura (2) and Withings (3). This was reflected in the frequency of low risk ratings too; the companies with the highest number of 'low risk' ratings were Google (17), Apple (15), Polar (15), Oura (13), Garmin (12) and Withings (12).

To illustrate each company's risk profile, we developed a heat map and calculated cumulative risk scores based on categorical ratings across the 24 rubric criteria. Each criterion was rated as High Risk (3 points), Some Concerns (2 points), or Low Risk (1 point), with a total possible score range of 24 (lowest risk) to 72 (highest risk). Xiaomi was identified as the highest risk company with a score of 60, and Google was identified as the lowest risk company with a score of 33. Table 2 presents these results, with companies ordered by overall risk score.

Table 1 | Evaluation of privacy practices in leading wearable device companies across 24 privacy criteria

		Apple	Coros	Fitbit	Fossil	Garmin	Google	Huawei	Oura	Polar	Samsung	Suunto	Ultrahuman	Wahoo	WHOOP	Withings	Wyze	Xiaomi
Transparency	1	1	3	1	2	2	3	3	1	3	2	3	2	1	3	1	3	3
	2	1	3	2	3	3	1	3	2	3	3	3	3	3	3	3	3	3
	3	1	3	2	2	3	1	3	3	3	3	3	1	3	2	3	2	2
	4	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1
Data Collection Purpose	5	1	1	2	1	1	1	3	1	1	1	3	2	2	3	1	3	3
	6	1	1	2	1	2	1	2	1	1	1	3	1	1	1	1	2	1
	7	1	1	2	2	1	2	3	1	1	2	2	2	2	3	2	3	3
	8	3	1	2	3	1	2	2	3	1	2	3	3	2	2	1	3	3
	9	2	2	2	1	1	3	1	1	1	2	2	2	3	3	1	3	3
Data minimisation	10	1	1	2	1	1	1	3	1	1	3	3	2	3	1	1	3	3
	11	1	2	1	2	1	2	2	1	1	2	2	2	3	2	2	2	3
	12	2	2	2	2	2	2	2	1	2	2	2	3	3	3	1	2	3
User Control and Rights	13	1	2	2	2	1	1	3	2	2	2	2	2	2	2	2	1	2
	14	1	1	2	1	2	1	2	2	1	1	1	1	1	1	1	2	3
	15	1	1	1	1	1	1	3	2	1	1	1	2	1	2	1	3	1
	16	2	2	1	2	1	1	3	1	1	1	3	2	2	3	1	2	3
Third Party Data Sharing	17	1	2	2	1	1	1	3	1	1	2	2	2	3	1	2	3	3
Data Security	18	1	3	1	3	1	1	1	2	1	2	3	1	3	2	1	3	1
	19	2	3	1	3	2	1	1	1	1	2	1	1	1	2	2	3	3
	20	2	3	2	3	2	1	3	1	2	2	1	2	2	2	2	3	3
	21	3	3	2	3	3	1	2	2	2	3	2	1	1	2	2	3	2
	22	1	3	3	3	3	1	1	2	1	1	2	2	3	1	2	1	3
	23	2	3	2	3	3	2	3	2	3	3	2	3	3	3	2	3	3
Breach notification	24	2	3	3	2	2	1	3	3	3	3	3	1	3	2	3	3	2

Companies in alphabetical order. Criteria in consecutive order as per the evaluation framework.

1 = Low risk; 2 = Some concerns; 3 = High risk. Each numbered criterion represents a specific privacy practice assessed across manufacturers:

1. User Notification About Third-Party Requests: Whether users are informed of data requests by governments or private entities, and if exceptions (e.g., gag orders) are disclosed.
2. Transparency Reporting: Availability of transparency reports detailing request counts, legal justifications, and affected users.
3. Threat Notification: Breach reporting procedures, including prompt notification to authorities and affected users.
4. Identity Policy: Whether users can register without presenting government-issued ID.
5. Data Use: Data is used only for explicitly stated purposes.
6. Data Collection: Clear disclosure of what data is collected, when, and whether third-party sources are involved.
7. Minimal Data Collection: Collection limited to essential data; non-essential permissions can be declined without impairing functionality.
8. Privacy by Default: Default settings prioritize privacy; targeted advertising is off by default.
9. Data Benefits: Benefits of data collection are clearly disclosed and user-oriented.
10. Purpose Limitation: Data is only collected and used for specified purposes.
11. User Control Over Data Collection: Users can restrict data collection while retaining product functionality.
12. Data Retention: Retention periods are disclosed; unnecessary data is deleted or anonymized.
13. Data Control: Users can limit data collection via in-app or account settings.
14. Control Over Targeted Advertising: Users can opt out of targeted ad tracking.
15. Data Access: Users can access personal data in a structured, portable format.
16. Data Deletion: Users can easily delete personal data; deletion policies are transparent.
17. Data Sharing: Disclosures about what data is shared, with whom, and why.
18. Authentication: Strong user authentication, including support for multi-factor methods.
19. Encryption: Data is encrypted in transit and at rest, ideally using end-to-end protocols.
20. Known Exploit Resistance: Evidence of protection against known vulnerabilities.
21. Security Oversight: Internal access controls and third-party audits are in place.
22. Security Over Time: Regular updates and communication about product security lifecycle.
23. Vulnerability Disclosure Program: Public bug reporting or bounty system, with defined resolution timelines.
24. Breach Notification: Clear, timely breach notification process for users and regulators.

The full evaluation results for each company across all 24 criteria are publicly available via the Open Science Framework (OSF) at: https://osf.io/vtwne/?view_only=1da176f8d0dc4574a454add4a4759c50.

Cluster analysis

Hierarchical cluster analysis using Ward's method identified three distinct clusters of wearable technology manufacturers based on their multi-dimensional privacy risk profiles.

Cluster 1 included Coros, Fossil, Oura, Fitbit, Withings, Polar, Garmin, and Samsung—companies that generally demonstrated moderate to low risk scores across most privacy dimensions. These manufacturers tended to provide reasonably clear privacy documentation, implement standard user control mechanisms, and showed some alignment with data minimisation and security best practices.

Cluster 2 consisted solely of Apple and Google, both of which were distinguished by notably strong performance across all dimensions. These companies consistently received Low Risk ratings on the majority of rubric criteria, describing comprehensive transparency practices, granular user controls, and robust approaches to data protection.

Cluster 3 included Suunto, Wahoo, Wyze, Huawei, Xiaomi, Whoop, and Ultrahuman, which clustered together due to higher overall privacy risk scores. These manufacturers commonly lacked sufficient transparency reporting, demonstrated weaker breach notification policies, and offered limited user control over data sharing and retention.

Table 2 | Aggregated privacy risk scores for 17 wearable device companies, ordered by total risk score and sorted by evaluation criteria in order of increasing frequency of 'high risk' ratings

		Evaluation Criteria																							
	Risk Score	13	4	6	14	15	11	7	16	17	19	20	5	12	9	10	18	21	22	1	3	8	24	23	2
Google	33	1	1	1	1	1	2	2	1	1	1	1	1	2	3	1	1	1	1	3	1	2	1	2	1
Apple	35	1	1	1	1	1	1	1	2	1	2	2	1	2	2	1	1	3	1	1	1	3	2	2	1
Oura	38	2	1	1	2	2	1	1	1	1	1	1	1	1	1	1	2	2	2	1	3	3	3	2	2
Polar	38	2	1	1	1	1	1	1	1	1	1	2	1	2	1	1	1	2	1	3	3	1	3	3	3
Withings	39	2	1	1	1	1	2	2	1	2	2	2	1	1	1	1	1	2	2	1	3	1	3	2	3
Garmin	41	1	1	2	2	1	1	1	1	1	2	2	1	2	1	1	1	3	3	2	3	1	2	3	3
Fitbit	43	2	1	2	2	1	1	2	1	2	1	2	2	2	2	2	1	2	3	1	2	2	3	2	2
Ultrahuman	44	2	1	1	1	2	2	2	2	2	1	2	2	3	2	2	1	1	2	2	1	3	1	3	3
Samsung	47	2	1	1	1	1	2	2	1	2	2	2	1	2	2	3	2	3	1	2	3	2	3	3	3
Fossil	48	2	1	1	1	1	2	2	2	1	3	3	1	2	1	1	3	3	3	2	2	3	2	3	3
Coros	50	2	1	1	1	1	2	1	2	2	3	3	1	2	2	1	3	3	3	3	3	1	3	3	3
Whoop	50	2	1	1	1	2	2	3	3	1	2	2	3	3	3	1	2	2	1	3	2	2	2	3	3
Wahoo	52	2	1	1	1	1	3	2	2	3	1	2	2	3	3	3	3	1	3	1	3	2	3	3	3
Suunto	53	2	1	3	1	1	2	2	3	2	1	1	3	2	2	3	3	2	2	3	3	3	3	2	3
Huawei	58	3	3	2	2	3	2	3	3	3	1	3	3	2	1	3	1	2	1	3	3	2	3	3	3
Wyze	60	1	1	2	2	3	2	3	2	3	3	3	3	2	3	3	3	3	1	3	2	3	3	3	3
Xiaomi	60	2	1	1	3	1	3	3	3	3	3	3	3	3	3	3	1	2	3	3	2	3	2	3	3

1 = Low risk; 2 = Some concerns; 3 = High risk.

Each numbered criterion represents a specific privacy practice or requirement, as outlined below:

1. User Notification About Third-Party Requests—The company informs users if governments or third parties request their data, including exceptions for legal restrictions.
2. Transparency Reporting—The company is transparent about data sharing, listing request numbers, legal bases, and affected accounts.
3. Threat Notification—The company promptly notifies authorities and users in the event of a data breach, detailing the response process.
4. Identity Policy—Users can register and use services without requiring government-issued ID for verification.
5. Data Use—Data is used only for the purposes for which it was collected, and all uses are disclosed to users.
6. Data Collection—The company discloses what data is collected, when it is collected, and whether third-party data is included.
7. Minimal Data Collection—Only essential data is collected; users can deny non-essential permissions without affecting functionality.
8. Privacy by Default—Privacy settings are configured optimally by default, and data collection for targeted advertising is off by default.
9. Data Benefits—Data collection benefits users, with clear disclosure of purposes for each data type collected.
10. Purpose Limitation—Data collected is limited to specific, disclosed purposes.
11. User Control Over Data Collection—Users can control what data is collected, and products function even if non-essential permissions are denied.
12. Data Retention—The company limits data retention, discloses retention periods, and deletes or anonymizes data when no longer necessary.
13. Data Control—Users can control data collection via settings, such as turning off collection or limiting permissions.
14. Control Over Targeted Advertising—Users can control and disable the use of their data for targeted advertising.
15. Data Access—Users can access their data easily, in a structured format, and at no cost.
16. Data Deletion—Users can delete their data, and the company provides clear deletion and retention policies.
17. Data Sharing—The company is transparent about data sharing, limiting it to necessary parties and disclosing what is shared and with whom.
18. Authentication—The company implements secure authentication mechanisms, such as multi-factor authentication, to protect user accounts.
19. Encryption—User data is encrypted during transmission and storage, with end-to-end encryption enabled by default.
20. Known Exploit Resistance—The product is secure against known vulnerabilities and exploits.
21. Security Oversight—The company monitors internal access to user data and commissions third-party security audits.
22. Security Over Time—The company ensures product security through regular updates and communicates the product lifecycle.
23. Vulnerability Disclosure Program—The company has a bug bounty or vulnerability disclosure program with clear timelines for addressing vulnerabilities.
24. Breach Notification—The company promptly notifies affected users and authorities in the event of a breach, with a clear process for addressing it.

This three-cluster typology illustrates the differentiation among manufacturers, with a clear distinction between industry leaders, privacy-conscious but mid-tier performers, and a group exhibiting substantive deficiencies in data governance.

Regional variations in privacy risk categories

Results of the chi-square test of independence revealed a significant association between geographical region and the distribution of privacy risk categories (χ^2 = 17.56, df = 4, $p = 0.002$). Post hoc analysis of standardized residuals showed that companies based in the Asia-Pacific region received significantly more High Risk ratings than expected (residual = +3.0) and significantly fewer Low Risk ratings (residual = −2.3). In contrast, North American and European companies exhibited distributions that did not deviate significantly from expected values, with no residuals exceeding ±2.0. These findings suggest that companies headquartered in Asia-Pacific are more likely to have higher privacy risks relative to their counterparts in North America and Europe.

Discussion

The primary aim of this study was to evaluate the privacy policies of leading wearable technology manufacturers, focusing on the ethical, legal, and transparency-related challenges associated with data collection and usage. To achieve this, we developed a bespoke evaluation framework designed to address gaps in existing standards and regulations. The framework assessed privacy practices across seven dimensions: transparency, data collection, data minimisation, user rights, third-party data sharing, data security, and breach notification. Each dimension was further broken down into 24 criteria informed by existing regulatory standards, industry guidelines, and best practices.

Our findings demonstrated substantial variability in privacy risk across the 17 companies assessed. While some companies adhered closely to best practices, others exhibited significant shortcomings, particularly in the domains of transparency reporting, vulnerability disclosure, and breach notification. For example, 76% of manufacturers were rated as High Risk for transparency reporting, 65% for vulnerability disclosure, and 59% for breach notification. The analysis also identified clear disparities among manufacturers, with Xiaomi, whose wearable devices are marketed under the Amazfit brand through its subsidiary Huami, receiving the highest number of High Risk ratings (16 out of 24 criteria). This was followed closely by Wyze (15) and Huawei (14).

The cluster analysis identified three main groupings: industry leaders (Apple and Google), mid-tier performers (Coros, Fossil, Oura, Fitbit, Withings, Polar, Garmin, and Samsung) and a group exhibiting substantive deficiencies in privacy protection (Suunto, Wahoo, Wyze, Huawei, Xiaomi, Whoop, and Ultrahuman). Google emerged as the overall leader in privacy protections, receiving the greatest number of Low Risk ratings (17) and an overall risk score of 33 (on a scale of 24–72, with higher scores indicating higher risk), while Xiaomi (Amazfit) was the worst-performing company, with a cumulative risk score of 60. Companies headquartered in Asia-Pacific demonstrated disproportionately higher frequencies of High Risk ratings, particularly in relation to transparency reporting and breach notification. In contrast, companies based in North America and Europe did not significantly deviate from expected distributions; their risk profiles were statistically similar, with relatively balanced frequencies of Low, Some concerns, and High Risk ratings.

Taken together, these findings highlight the regulatory gaps in addressing the unique privacy challenges posed by wearable technologies and the potential risks to users from inconsistent data practices. The absence of consistent, enforceable global standards leaves consumers vulnerable to opaque data-sharing practices, insufficient security measures, and inadequate protections for sensitive health biodata. While consumer advocacy groups such as the Digital Standard and Mozilla Foundation's Privacy Not Included initiative provide valuable tools for evaluating consumer-facing technologies—and informed aspects of our rubric—they are generalised frameworks that do not account for the distinct privacy challenges associated with wearable-derived biometric data. Similarly, existing regulatory frameworks, including the GDPR, CCPA, and HIPAA, offer robust protections for user data but were not designed to address the continuous data streams, complex third-party ecosystems, and pervasive data collection intrinsic to wearable technologies. These gaps, coupled with the lack of global regulatory harmonisation, underscore the urgent need for a targeted approach tailored to wearable technologies, one that integrates principles of privacy, fairness, and accountability into their development and governance. To support these efforts, we have provided a series of targeted recommendations for each company, detailing how they can improve their practices across the seven dimensions and 24 criteria assessed in this study.

The widespread adoption of wearable technologies and their integration into large-scale research initiatives highlight their transformative potential for both personal health management and public health research. For instance, wearable-derived data has been leveraged to predict COVID-19 diagnoses[47], monitor influenza outbreaks in real time[15,48], and assess socioeconomic trends[49]. Prominent research initiatives, such as the National Institutes of Health's *All of Us* program[50] and the UK's *Our Future Health* project[51] involve hundreds of thousands of participants and use wearable data to inform personalised health strategies and public health interventions. Similarly, studies conducted by the Scripps Research Translational Institute illustrate the value of wearables in tracking population health metrics and detecting early signs of viral illnesses[47,52,53]. These initiatives exemplify a paradigm shift in the role of wearable technologies, demonstrating their capacity to extend beyond individual fitness tracking into broader scientific, clinical, and public health domains.

However, the increasing prominence of wearable-derived data in research and public domains amplifies the associated privacy and security risks. Each wearable device continuously collects thousands of data points per user per day[5]. Over time, the cumulative data volume becomes vast, yet much of it is collected and processed without users' explicit understanding or control. Previous research has highlighted risks stemming from inadequate data protection, opaque third-party sharing practices, and regulatory gaps that leave users vulnerable to breaches[33,42,54]. Informed consent—a cornerstone of ethical data collection—is often undermined by lengthy and complex privacy policies, which in this review averaged 6113 words and would take approximately 26 min to read[55]. Unsurprisingly, up to 97% of users accept these agreements without fully understanding their terms[32,43]. Once accepted, these agreements often grant manufacturers broad discretion to share data with third parties or store it in jurisdictions with weaker privacy protections[33,56].

These challenges are magnified when considering the disproportionate harms that wearable surveillance can impose on vulnerable populations. For example, studies have shown that heart rate sensors on some wearables are less accurate for individuals with darker skin tones[57], reflecting a racial design bias that may affect health outcomes. Meanwhile, law enforcement agencies in the U.S. and other jurisdictions have purchased commercial data —including from wearables—to conduct location tracking, raising concerns about discriminatory surveillance of racial and ethnic minorities[58]. Such practices echo broader concerns about the use of biometric data in predictive policing models, which risk replicating existing biases under the guise of algorithmic objectivity[59,60].

Children and adolescents are another group at heightened risk. Wearables marketed to minors frequently collect geolocation, audio, and health data with minimal parental awareness or consent, and in some cases have been found to act as de facto surveillance devices[61]. A notable example includes Germany's ban on certain children's smartwatches, which were found to function as covert listening tools, violating both child protection laws and parental trust[62]. Similarly, older adults, who may rely on wearables for fall detection or chronic disease monitoring[63], are often unaware of how their data is shared with insurers or third parties[64]—raising the possibility of discrimination in premiums or coverage based on wearable-derived metrics.

The risks associated with these practices are compounded by the increasing frequency and sophistication of data breaches. Consumer data stored in the cloud is a prime target for hackers, who are increasingly focusing on sensitive information such as government, genetic, and healthcare data[65,66]. Alarmingly, 98% of organisations have a relationship with at least one vendor that has experienced a data breach, reflecting the vulnerability introduced by third-party dependencies[66]. This is particularly concerning for wearable device companies, which commonly share consumer data with affiliates or external vendors. For example, a 2021 breach of a third-party platform that allowed users to sync health and fitness data compromised the records of 61 million Fitbit and Apple users[34]. Although not directly caused by these manufacturers, the incident illustrates the risks inherent in third-party data sharing.

The issue is not solely technological. Structural factors such as vendor lock-in and 'choice legacy'—where users become dependent on proprietary software ecosystems—further reduce users' ability to manage or transfer their data[4,33]. This entrenches an imbalance of power between the company and the customer, reducing opportunities for meaningful user autonomy and perpetuating ecosystems where privacy concerns may persist. Combined with the limited adoption of robust security measures—encryption procedures were described in 47% of the privacy policies we reviewed—this dynamic increases the potential for data misuse.

In the future, the collection and utilisation of biometric data are likely to transcend commercial interests, carrying profound implications for the relationship between the state and its citizens. Governments are increasingly leveraging biometric data beyond public health, including in national security, immigration, and criminal justice contexts[67,68]. Without strict oversight, the integration of wearable data into state surveillance infrastructures could erode anonymity and civil liberties, particularly for marginalized communities. Predictive policing, algorithmic bias in health systems, and biometric-based nudging of user behaviour all point toward a future in which personal autonomy is at risk of being algorithmically constrained[26,69–71]. These developments require ethical scrutiny, robust legal protections, and strong governance frameworks that centre on fairness, equity, and user dignity.

Within the scope of this review, several areas for improvement were identified, including the standardisation of privacy policies, enhanced user control mechanisms, stronger privacy defaults, and stricter accountability measures for data handling. Privacy policies must transition from their current state—dominated by dense, opaque legal jargon—into concise, accessible, and interactive documents that users can easily navigate. However, given well-documented behavioural barriers such as consent fatigue and privacy paradox effects, improving disclosure alone will not be sufficient. Privacy-protective default settings should be implemented, ensuring that users are automatically granted the highest reasonable level of privacy unless they actively choose otherwise. Additionally, manufacturers should offer users simplified privacy 'types' or profiles during device setup (e.g., 'Maximal Privacy,' 'Balanced,' or 'Performance Optimized'), enabling informed customization without overwhelming users with granular settings. These measures, rooted in principles of Privacy by Design and Privacy by Default, could meaningfully enhance user autonomy and trust. Importantly, adherence to these policies and settings must be subject to continual evaluation.

Herein lies the primary limitation with this review: policy does not necessarily reflect practice. While privacy policies remain the public-facing cornerstone of companies' data commitments, real-world behaviour often diverges from what is disclosed—either through omission, ambiguity, or outright misrepresentation. This gap between declared policy and operational reality has become increasingly visible in recent years, even among companies that scored well in our evaluation. For example, Apple, widely marketed as privacy-centric and rated in the 'low risk' cluster in our synthesis, settled a $95 million class-action lawsuit in 2025 over its Siri voice assistant's undisclosed recording of user conversations via accidental activations on Apple Watches and other devices[72]. Despite public assurances, Apple's privacy policy at the time failed to explicitly disclose that human contractors would review audio recordings—highlighting the limits of written policy in predicting actual data flows.

Similarly, Google—which also received strong scores in our analysis—faced legal action after investigations revealed that it continued tracking user location data even after users had disabled the 'Location History' setting. Regulators across 40 U.S. states reached a $391.5 million settlement with Google in 2022, citing deceptive privacy controls that misled users into thinking they had opted out of tracking[73]. This misalignment between interface, policy, and practice exposed users of Wear OS devices and Fitbit products—now owned by Google—to significant privacy risks. Fitbit, in particular, illustrates the operational vulnerabilities of wearable companies. In 2023, the privacy advocacy group NOYB filed GDPR complaints in three EU jurisdictions, arguing that Fitbit's mandatory consent for international data transfers (with no real opt-out aside from account deletion) violated fundamental principles of freely given and withdrawable consent[74]. Despite ostensibly compliant privacy policies, the company's actual data-sharing practices and lack of transparency regarding health data transfers revealed serious regulatory concerns.

Collectively, these cases underscore that even robust public policies are insufficient safeguards without accompanying operational transparency and compliance mechanisms. Future research must prioritise 'living' assessments that track not just what companies *say* they do with user data, but what they actually do—across codebases, server logs, subcontractor relationships, and enforcement actions. Transparency reporting should also become a standard industry obligation, not an optional goodwill gesture. Manufacturers should regularly disclose the volume and nature of third-party data requests, the legal basis for each, and their rates of compliance. Additionally, fostering greater interoperability across wearable ecosystems could mitigate the privacy and autonomy risks associated with 'choice legacy,' allowing users to retain access to historical health data irrespective of vendor lock-in or platform migration.

Taken together, these measures—operational transparency, regulatory accountability, user-centred design, and interoperability—represent a pathway to realigning the wearable technology sector with principles of fairness, accountability, and respect for individual rights in an era of pervasive biometric surveillance.

Methods

To assess the privacy practices of consumer wearable technology manufacturers, we developed a tailored privacy and data security rubric. This framework focused on ethical, legal, and transparency-related challenges associated with the collection, use, and protection of user data.

Evaluation framework design process

The Privacy and Data Security Evaluation Framework was developed through a multi-step, evidence-driven process involving expert consultation, regulatory analysis, and pilot testing. Recognising that existing frameworks—including the GDPR[36], CCPA[38], the Digital Standard[45], the methodology employed by Mozilla's Privacy Not Included team[44], and general OECD privacy principles—are not sufficiently tailored to the specific characteristics of consumer wearable technologies (e.g., continuous biometric monitoring, app-device integrations, and proprietary cloud ecosystems), we created a purpose-built rubric informed by legal and ethical standards.

Development began with a comprehensive review of global regulatory frameworks (GDPR, CCPA, HIPAA, NIST, ISO/IEC 27001, and others), digital ethics benchmarks (FIPPs, UN Digital Identity Principles), and consumer privacy initiatives. Specific articles and provisions—such as GDPR Articles 5, 15, 17, 20, 25, and 32; CCPA Sections 1798.110, 1798.120, 1798.135; and NIST SP 800-61—were mapped to indicators that collectively shaped our framework.

Stakeholder engagement consisted of structured expert input from privacy, consumer rights, and cybersecurity specialists. This included collaboration with Mozilla's Privacy Not Included team, as well as consultations with our University's Data Protection Officer and legal team. While we did not conduct formal participatory workshops with consumers, this decision reflects the highly technical nature of the policy language under review and the normative structure of privacy compliance rubrics, which are grounded in legal obligations rather than preference elicitation.

A preliminary version of the rubric was piloted on a representative sample of privacy policies from major wearable device manufacturers. This phase tested clarity, consistency, and discriminatory capacity across rubric dimensions and informed revisions to improve operational precision. The final rubric comprised seven dimensions:

1. *Transparency*
2. *Data Collection Purposes*
3. *Data Minimisation*
4. *User Control and Rights*
5. *Third-Party Data Sharing*
6. *Data Security*
7. *Breach Notification*

Each dimension included multiple evaluation criteria, with defined indicators grounded in specific regulatory sources (see Table 3). A detailed rubric, source mapping, and policy rating definitions are provided in Supplemental File 1.

Collation of consumer wearable device company privacy policies

We identified companies for evaluation using a 2024 Statista report, which ranked leading wearable device manufacturers based on global market share[1]. From this list, we selected the top 10 companies, ensuring representation of key market leaders with substantial user bases. To broaden the scope of our analysis, we supplemented this selection with smaller or emerging manufacturers that cater to niche markets or demonstrate innovative privacy and data handling practices.

The selected companies represented diverse geographical regions, including North America, Europe, and Asia-Pacific. For each company, we retrieved the most recent publicly available privacy policies from official websites or customer support pages between September 2024 and May 2025. Where companies provided different privacy policies or region-specific addenda for users in the European Union, United States, or other jurisdictions, each version was retrieved, reviewed, and evaluated separately to account for jurisdictional differences in privacy practices, however, we only included the global policies in this analysis.

Table 3 | Privacy and data security evaluation framework for wearable technologies

Dimension	Criterion	Indicators	Source regulation or framework
1. Transparency	User Notification About Third-Party Requests for User Information	1. User notification for government requests 2. User notification for private requests 3. Disclosure of non-notification scenarios (e.g., legal restrictions)	GDPR Art. 15(1)(g), CCPA 1798.110(c)
	Transparency Reporting	1. Number of requests by country 2. Request types (stored info, real-time) 3. Accounts affected 4. Legal basis disclosed	Digital Standard, GDPR Art. 12, GDPR Recital 63
	Threat Notification	1. Prompt authority notification for breaches 2. User notification process 3. Breach handling procedures	GDPR Art. 33, CCPA 1798.82, NIST SP 800-61
	Identity Policy	1. No requirement for government-issued ID verification	UN Digital Identity Principles, GDPR Art. 5 (data minimization), OECD Privacy Principles
2. Data Collection Purpose	Data Use	1. Data usage limited to the collection purpose 2. Disclosure of all data uses	GDPR Art. 5(1)(b), OECD Privacy Principles
	Data Collection	1. Specific data elements disclosed 2. Collection method and timing 3. Inclusion of third-party data	CCPA 1798.110(a), GDPR Art. 13(1)(c), Digital Standard
	Minimal Data Collection	1. Commitment to minimal data collection 2. Product functionality without unnecessary permissions	GDPR Art. 5(1)(c) (Data Minimization), Digital Standard, HIPAA Minimum Necessary Standard
	Privacy by Default	1. Default optimal privacy settings 2. Targeted advertising off by default	GDPR Art. 25, Digital Standard
	Data Benefits	1. Purpose disclosure for each data type	Fair Information Practice Principles (FIPPs), Digital Standard
3. Data Minimization	Purpose Limitation	1. Data collection purpose specified 2. Only necessary data collected	GDPR Art. 5(1)(b), HIPAA
	User Control Over Data Collection	1. Data collection controls 2. Functionality with disabled non-essential permissions	GDPR Art. 20, CCPA 1798.105, Digital Standard
	Data Retention	1. Retention period disclosure 2. Data deletion or anonymization when not necessary	GDPR Art. 5(1)(e), CCPA 1798.105(c), HIPAA
4. User Control and Rights	Data Control	1. Ability to disable or limit data collection 2. Controls via website/app	CCPA 1798.135, GDPR Art. 20
	Control Over Targeted Advertising	1. Option to disable targeted advertising	CCPA 1798.120, GDPR Art. 21
	Data Access	1. Disclosure of accessible data types 2. Structured format (e.g., JSON, CSV)	GDPR Art. 15, CCPA 1798.100(d)
	Data Deletion	1. Retention period disclosure 2. Easy deletion of non-essential data	CCPA 1798.105(a), GDPR Art. 17 (Right to Erasure)
5. Third-Party Data Sharing	Data Sharing	1. Scope and necessity of data sharing 2. Disclosure of shared data and recipients 3. Disclosure of government sharing	GDPR Art. 5(1)(c), CCPA 1798.115(a), Digital Standard
6. Data Security	Authentication	1. Multi-factor authentication available 2. Authentication required per access 3. Brute-force resistance	NIST SP 800-63, GDPR Art. 32
	Encryption	1. Transmission and storage encryption 2. Default end-to-end encryption	GDPR Art. 32, HIPAA
	Known Exploit Resistance	1. Security against known bugs and attacks	OWASP Top Ten, ISO/IEC 27001, NIST
	Security Oversight	1. Internal access limits and monitoring 2. Third-party audits	ISO/IEC 27001, GDPR Art. 24
	Security Over Time	1. Lifecycle communication 2. Automatic updates	NIST SP 800-128, GDPR Art. 32
	Vulnerability Disclosure Program	1. Bug bounty or vulnerability disclosure 2. Timeframe for addressing vulnerabilities	Digital Standard, ISO/IEC 29147
7. Breach Notification	Threat Notification	1. Prompt authority notification 2. User breach notification and response details	GDPR Art. 33, CCPA 1798.82, NIST SP 800-61

Table 3 (continued) | Privacy and data security evaluation framework for wearable technologies

Dimension	Criterion	Indicators	Source regulation or framework

GDPR (General Data Protection Regulation): EU regulation (Regulation (EU) 2016/679) harmonizing data privacy laws across Europe with emphasis on user rights and data protection. Relevant articles:
- Art. 5: Core principles of data processing, including purpose limitation and minimization.
- Art. 15: Right of access to personal data.
- Art. 17: Right to erasure ('right to be forgotten').
- Art. 20: Right to data portability.
- Art. 25: Privacy by design and default.
- Art. 32: Security of processing.
- Art. 33: Breach notification to authorities.

CCPA (California Consumer Privacy Act): California law granting consumers rights over their personal information. Key sections:
- §1798.105: Right to delete personal data.
- §1798.110: Right to know what data is collected/shared.
- §1798.115: Right to know about third-party sharing.
- §1798.120: Right to opt out of data sale.
- §1798.135: Mandatory 'Do Not Sell My Info' link.
- §1798.82: Breach notification requirements.

NIST (National Institute of Standards and Technology): U.S. agency issuing cybersecurity standards. Key publications:
- SP 800-61: Incident response guidance.
- SP 800-63: Digital identity and authentication.
- SP 800-128: Configuration management.

ISO/IEC Standards:
- ISO/IEC 27001: Information security management systems (ISMS).
- ISO/IEC 29147: Vulnerability disclosure procedures.

HIPAA (Health Insurance Portability and Accountability Act): U.S. law regulating health information privacy.

OECD Privacy Principles: International guidelines promoting fair, transparent data practices.

OWASP Top Ten: A ranked list of critical web application security risks from the Open Web Application Security Project.

FIPPs (Fair Information Practice Principles): Widely adopted privacy principles including transparency, control, and data minimization.

UN Digital Identity Principles: UN guidelines ensuring digital identity systems protect fundamental rights, including privacy and anonymity.

Digital Standard: A consumer-focused set of privacy and security benchmarks developed by Consumer Reports and Mozilla.

Procedures for evaluation

Privacy policies were assessed through a structured three-step process using the evaluation rubric, with two independent reviewers assessing each policy version:

1. Document Analysis: Reviewers systematically analysed privacy policies, terms of service, and transparency reports for evidence matching rubric indicators. For example, under the 'Transparency Reporting' criterion, policies were examined for disclosure of the number of government data requests, affected user accounts, and the legal basis for such disclosures.
2. Rating Assignment: Each criterion was assigned one of three ratings: 1) High Risk: Reflects missing or poor practices posing direct risks to user privacy (e.g., no third-party disclosure information, lack of encryption, absence of breach reporting procedures). 2) Low Risk: Indicates strong adherence to regulatory standards and user-centric design (e.g., clear data deletion pathways, opt-out controls for advertising, published vulnerability disclosure policies). 3) Some Concerns: Assigned where policy language was ambiguous or failed to address the criterion (e.g., undefined data retention periods, vague references to 'partners'). Each rating decision was supported by direct excerpts from the policy text and assessed according to the definitions and examples provided in our rubric (see Evaluation Rating Definitions in Supplemental File 1).
3. Recommendation Generation: For any criterion rated High Risk or Some concerns, tailored improvement recommendations were developed referencing the relevant legal and ethical standards.

Living review implementation

Given the dynamism of the wearable technology sector and the evolving landscape of privacy regulations and data governance practices, we plan to maintain this evaluation as a living review. Updates will be conducted through regular monitoring of privacy policies from the original cohort of manufacturers. We will perform systematic checks every 6 months, retrieving and reviewing any newly issued or updated privacy policies from these companies. Where substantive changes are identified, the same evaluation rubric and rating procedures described in this manuscript will be applied. Updated assessments will be synthesised with prior findings to reflect changes over time in company privacy practices. Review updates will be uploaded to an open-access repository on OSF.io (https://osf.io/vtwne/?view_only=1da176f8d0dc4574a454add4a4759c50). Each update will constitute a new version of the living review, with a unique identifier and a comprehensive changelog documenting all modifications relative to the previous version. All versions will remain publicly accessible, allowing readers to trace the evolution of privacy protections across the wearable technology sector.

Statistical analysis

Reliability analysis for inter-rater agreement. To evaluate the reliability of the rubric and the consistency of ratings, we conducted an inter-rater reliability analysis using two independent raters. Both raters received training to ensure uniform understanding of criteria, indicators, and rating categories (High Risk, Some Concerns, Low Risk). Calibration exercises were conducted using practice policies to address discrepancies and standardise the application of the rubric.

Raters independently evaluated the same policies, and inter-rater reliability was assessed using Cohen's Kappa. Agreement levels were interpreted as follows: >0.80: Excellent agreement, indicating robust rubric clarity; 0.60–0.80: Substantial agreement, suggesting minor refinements might improve consistency; 0.40–0.60: Moderate agreement, highlighting the need for further clarification; <0.40: Low agreement, indicating significant ambiguity. Discrepancies between raters were resolved through discussion, with finalised ratings used for subsequent analyses.

Analysis of privacy policy ratings. We performed descriptive analyses to summarise the distribution of privacy risk ratings across the seven rubric dimensions. For each dimension, we calculated the percentage of policies rated as High Risk, Some Concerns, or Low Risk. Results were visually represented using risk matrices, allowing for comparisons between companies and highlighting dimension-specific vulnerabilities.

We supplemented this with a hierarchical cluster analysis to identify natural groupings of companies based on their privacy risk profiles. Risk scores across 24 evaluation criteria were used as input variables. Clustering was performed using Ward's method with squared Euclidean distance as the similarity measure. Inspection of the agglomeration schedule and dendrogram was used to select the cluster solution.

Finally, to explore potential regional differences, companies were grouped by headquarters location (North America, Europe, Asia-Pacific). A Chi-Square Test of Independence was used to evaluate associations between geographical region and privacy risk ratings. Post hoc analysis of standardised residuals (≥ ±2.0) was used to identify significant deviations from expected distributions.

All statistical analyses were conducted using SPSS (version 29), with a significance level of 0.05.

Data availability

The data supporting the findings of this study are openly available on the Open Science Framework (OSF) at: https://osf.io/vtwne/?view_only=1da176f8d0dc4574a454add4a4759c50. The repository includes: Archived versions of privacy policies from 17 leading wearable technology manufacturers. A version-tracking log detailing which policy version was reviewed, when it was collected, and whether more recent versions exist.The full evaluation rubric used to assess privacy practices including regulatory sources and scoring indicators.Completed company-level evaluations across 24 privacy and security criteria.Supplementary materials including risk matrices and inter-rater reliability outputs. All data have been structured to support reproducibility and transparency, and the repository will be updated annually as part of an ongoing 'living review' model.

Received: 10 February 2025; Accepted: 27 May 2025;
Published online: 14 June 2025

References

1. Statista. Wearables Statista Dossier. (2024).
2. Dunn, J., Runge, R. & Snyder, M. Wearables and the medical revolution. *Pers. Med.* **15**, 429–448 (2018).
3. Piwek, L., Ellis, D. A., Andrews, S. & Joinson, A. The rise of consumer health wearables: promises and barriers. *PLoS Med.* **13**, e1001953 (2016).
4. Doherty, C., Baldwin, A., Argent, R., Keogh, A. & Caulfield, B. Keeping pace with wearables: a living umbrella review of systematic reviews evaluating the accuracy of commercial wearable technologies in health measurement. *Sports Med.* **54**, 2907-2926 (2024).
5. Ash, G. I. et al. Establishing a global standard for wearable devices in sport and exercise medicine: perspectives from academic and industry stakeholders. *Sports Med.* **51**, 2237–2250 (2021).
6. Keogh, A. et al. Six-month pilot testing of a digital health tool to support effective self-care in people with heart failure: mixed methods study. *JMIR Form. Res.* **8**, e52442 (2024).
7. Franssen, W. M. A., Franssen, G., Spaas, J., Solmi, F. & Eijnde, B. O. Can consumer wearable activity tracker-based interventions improve physical activity and cardiometabolic health in patients with chronic diseases? A systematic review and meta-analysis of randomised controlled trials. *Int. J. Behav. Nutr. Phys. Act.* **17**, 57 (2020).
8. Brickwood, K. J., Watson, G., O'Brien, J. & Williams, A. D. Consumer-based wearable activity trackers increase physical activity participation: systematic review and meta-analysis. *JMIR Mhealth Uhealth* **7**, e11819 (2019).
9. Beck, A. J. et al. Using wearable and mobile technology to measure and promote healthy sleep behaviors in adolescents: a scoping review protocol. *JBI Evid. Synth.* **19**, 2760–2769 (2021).
10. Chong, K. P. L., Guo, J. Z., Deng, X. & Woo, B. K. P. Consumer perceptions of wearable technology devices: retrospective review and analysis. *JMIR Mhealth Uhealth* **8**, e17544 (2020).
11. Düking, P. et al. Monitoring and adapting endurance training on the basis of heart rate variability monitored by wearable technologies: a systematic review with meta-analysis. *J. Sci. Med. Sport* **24**, 1180–1192 (2021).
12. Camomilla, V., Bergamini, E., Fantozzi, S. & Vannozzi, G. Trends supporting the in-field use of wearable inertial sensors for sport performance evaluation: a systematic review. *Sensors* **18**, 873 (2018).
13. Longhini, J. et al. Wearable devices to improve physical activity and reduce sedentary behaviour: an umbrella review. *Sports Med. Open* **10**, 9 (2024).
14. Laranjo, L. et al. Do smartphone applications and activity trackers increase physical activity in adults? Systematic review, meta-analysis and metaregression. *Br. J. Sports Med.* **55**, 422–432 (2021).
15. Radin, J. M., Wineinger, N. E., Topol, E. J. & Steinhubl, S. R. Harnessing wearable device data to improve state-level real-time surveillance of influenza-like illness in the USA: a population-based study. *Lancet Digit. Health* **2**, e85–e93 (2020).
16. Moshawrab, M., Adda, M., Bouzouane, A., Ibrahim, H. & Raad, A. Smart wearables for the detection of cardiovascular diseases: a systematic literature review. *Sensors* **23**, 828 (2023).
17. Sarwar, A., Agu, E. O. & Almadani, A. CovidRhythm: a deep learning model for passive prediction of COVID-19 using biobehavioral rhythms derived from wearable physiological data. *IEEE Open J. Eng. Med. Biol.* **4**, 21–30 (2023).
18. Alavi, A. et al. Real-time alerting system for COVID-19 and other stress events using wearable data. *Nat. Med.* **28**, 175–184 (2022).
19. Polonelli, T., Schulthess, L., Mayer, P., Magno, M. & Benini, L. H-Watch: an open, connected platform for AI-enhanced CoViD19 infection symptoms monitoring and contact tracing. in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)* 1-5 (IEEE, 2021).
20. Koch, M. et al. Wearables for measuring health effects of climate change-induced weather extremes: scoping review. *JMIR Mhealth Uhealth* **10**, e39532 (2022).
21. Barteit, S. et al. Feasibility, acceptability and validation of wearable devices for climate change and health research in the low-resource contexts of Burkina Faso and Kenya: Study protocol. *PLoS One* **16**, e0257170 (2021).
22. Doherty, C. et al. An Evaluation of the effect of app-based exercise prescription using reinforcement learning on satisfaction and exercise intensity: randomized crossover trial. *JMIR Mhealth Uhealth* **12**, e49443 (2024).
23. Shajari, S., Kuruvinashetti, K., Komeili, A. & Sundararaj, U. The emergence of ai-based wearable sensors for digital health technology: a review. *Sensors* **23**, 9498 (2023).
24. Olyanasab, A. & Annabestani, M. Leveraging machine learning for personalized wearable biomedical devices: a review. *J. Pers. Med.* **14**, 203 (2024).
25. Sivakumar, C. L. V., Mone, V. & Abdumukhtor, R. Addressing privacy concerns with wearable health monitoring technology. *WIREs Data Min. Knowl. Discov.* **14**, e1535 (2024).
26. Keserű, J. From skin to screen: bodily integrity in the digital age. (Mozilla Foundation, 2024).
27. Neumann, D., Tiberius, V. & Biendarra, F. Adopting wearables to customize health insurance contributions: a ranking-type Delphi. *BMC Med. Inform. Decis. Mak.* **22**, 112 (2022).
28. Brassart Olsen, C. To track or not to track? Employees' data privacy in the age of corporate wellness, mobile health, and GDPR†. *Int. Data Priv. Law* **10**, 236–252 (2020).
29. Ibarra, J., Jahankhani, H. & Kendzierskyj, S. Cyber-physical attacks and the value of healthcare data: facing an era of cyber extortion and organised crime. *Blockchain Clin. Trial* 115–137 (2019).
30. Imprivata. Hackers, breaches, and the value of healthcare data. https://www.imprivata.com/uk/node/103708 (2021).
31. Choi, J. P., Jeon, D.-S. & Kim, B.-C. Privacy and personal data collection with information externalities. *ISN: Property Protection (Topic)* (2018).
32. Milne, G. R. & Culnan, M. J. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *J. Interact. Mark.* **18**, 15–29 (2004).

33. Schumann, M. & Doherty, C. Bridging gaps in wearable technology for exercise and health professionals: a brief review. *Int. J. Sports Med.* **45**, 949-957 (2024).
34. Osborne, C. Over 60 million wearable, fitness tracking records exposed via unsecured database. https://www.zdnet.com/article/over-60-million-records-exposed-in-wearable-fitness-tracking-data-breach-via-unsecured-database/ (2022).
35. Abrams, L. UnitedHealth says data of 100 million stolen in Change Healthcare breach. in *Bleeping Computer* (2024).
36. Wolford, B. What is GDPR, the EU's new data protection law? (GDPR.eu, 2024).
37. Services, U.S.D.o.H.a.H. Health Insurance Portability and Accountability Act of 1996 (HIPAA) (2024).
38. California Department of Justice, O.o.t.A.G. California Consumer Privacy Act (CCPA, 2024).
39. Canada, O.o.t.P.C.o. The Personal Information Protection and Electronic Documents Act (PIPEDA, 2021).
40. (CBPR), A.C.-B.P.R. CBPR Policies, Rules and Guidelines (Revised for Posting 3-16, Updated 2019) (2019).
41. Zhang, C., Shahriar, H. & Riad, A. B. M. K. Security and Privacy Analysis of Wearable Health Device. in *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)* 1767-1772 (2020).
42. Cilliers, L. Wearable devices in healthcare: privacy and information security issues. *Health Inf. Manag* **49**, 150–156 (2020).
43. Steinfeld, N. "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Comput. Hum. Behav.* **55**, 992–1000 (2016).
44. Foundation, M. Privacy Not Included. (2024).
45. Reports, C. The Digital Standard. (2024).
46. Rights, N.-E.C.f.D. NOYB Enforces Your Right to Privacy Every Day. (2024).
47. Radin, J. M. et al. Sensor-based surveillance for digitising real-time COVID-19 tracking in the USA (DETECT): a multivariable, population-based, modelling study. *Lancet Digit. Health* **4**, e777–e786 (2022).
48. González, M. C., Hidalgo, C. A. & Barabási, A. L. Understanding individual human mobility patterns. *Nature* **453**, 779–782 (2008).
49. Blumenstock, J., Cadamuro, G. & On, R. Predicting poverty and wealth from mobile phone metadata. *Science* **350**, 1073–1076 (2015).
50. Denny, J. C. et al. The "All of Us" research program. *N. Engl. J. Med.* **381**, 668–676 (2019).
51. Evidation. Evidation Selected by Our Future Health as Participant Platform for UK's Largest Health Research Program. (2023).
52. Gadaleta, M. et al. Passive detection of COVID-19 with wearable sensors and explainable machine learning algorithms. *npj Digit. Med.* **4**, 166 (2021).
53. Quer, G. et al. Wearable sensor data and self-reported symptoms for COVID-19 detection. *Nat. Med.* **27**, 73–77 (2021).
54. de Arriba-Perez, F., Caeiro-Rodriguez, M. & Santos-Gago, J. M. Collection and processing of data from wrist wearable devices in heterogeneous and multiple-user scenarios. *Sensors* **16**, 1538 (2016).
55. Brysbaert, M. How many words do we read per minute? A review and meta-analysis of reading rate. *J. Mem. Lang.* **109**, 104047 (2019).
56. Keogh, A. et al. Breaking down the digital fortress: the unseen challenges in healthcare technology-lessons learned from 10 years of research. *Sensors* **24**, 3780 (2024).
57. Koerber, D., Khan, S., Shamsheri, T., Kirubarajan, A. & Mehta, S. Accuracy of heart rate measurement with wrist-worn wearable devices in various skin tones: a systematic review. *J. Racial Ethn. Health Disparities* **10**, 2676-2684 (2022).
58. Toomey McKenna, A. US agencies buy vast quantities of personal information on the open market–a legal scholar explains why and what it means for privacy in the age of AI. in *The Conversation* (2023).
59. Gilmore, J. N. & Gruber, C. Wearable witnesses: Deathlogging and framing wearable technology data in "Fitbit murders". *Mob. Media Commun.* **12**, 195–211 (2024).
60. Hung, T.-W. & Yen, C.-P. Predictive policing and algorithmic fairness. *Synthese* **201**, 206 (2023).
61. Shi, M. Who's Really Watching? The Hidden Data Risks of Children's "Phone Watches". (Responsible Data for Children, 2024).
62. Reuters. German agency bans children's 'smart' watches over spying concerns (2017).
63. Moore, K. et al. Older adults' experiences with using wearable devices: qualitative systematic review and meta-synthesis. *JMIR Mhealth Uhealth* **9**, e23832 (2021).
64. Kim, T. K. & Choi, M. Older adults' willingness to share their personal and health information when adopting healthcare technology and services. *Int. J. Med. Inform.* **126**, 86–94 (2019).
65. Madnick, S. E. The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase. Apple. https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to …, (2023).
66. Pitrelli, M. Leaked documents show notorious ransomware group has an HR department, performance reviews and an 'employee of the month'. *CNBC, April* **13** (2022).
67. Mennella, C., Maniscalco, U., De Pietro, G. & Esposito, M. Ethical and regulatory challenges of AI technologies in healthcare: a narrative review. *Heliyon* **10**, e26297 (2024).
68. Parliament, U.K. The Impact of Biometric Data in Government Policy. (2023).
69. Angwin, J., Larson, J., Mattu, S. & Kirchner, L. Machine bias. in *Ethics of data and analytics* 254-264 (Auerbach Publications, 2022).
70. Eubanks, V. *Automating inequality: How high-tech tools profile, police, and punish the poor*, (St. Martin's Press, 2018).
71. Rahman, Z. & Keseru, J. *Predictive Analytics for Children: An assessment of ethical considerations, risks, and benefits*, (UNICEF Office of Research-Innocenti, 2021).
72. Stempel, J. Apple to pay $95 million to settle Siri privacy lawsuit. (Reuters, 2025).
73. Bartz, D., Shepardson, D. & Freifeld, K. Google to pay nearly $400 million to settle U.S. location-tracking probe. (Reuters, 2022).
74. Mukherjee, S. Privacy activist Schrems files complaints against Google's Fitbit. (Reuters 2023).

Acknowledgements

This publication has emanated from research conducted with the financial support of the Health Research Board in Ireland (Grant ID: HRB ILP-PHR-2024-005) and Research Ireland (12/RC/2289_P2).

Author contributions

C.D. conceptualised the study, developed the methodology and evaluation framework (with industry partners), and conducted the review of company privacy policies—leading the formal analysis. They also contributed to data interpretation and supervised the overall study design. M.B. developed the methodology and evaluation framework and conducted the review of company privacy policies. They also contributed to data interpretation and manuscript drafting. R.L. contributed to investigation, resources, and methodology refinement. M.A. contributed to the investigation and formal analysis. They provided expertise in wearable technology data privacy and assisted in refining the evaluation framework. B.C. supervised the study, provided oversight on methodology and data analysis, and contributed to writing—review and editing. All authors contributed to writing—review and editing and approved the final manuscript.

Competing interests

The authors declare no competing interests. No author has received personal or financial support from any of the companies evaluated in this study. The research was conducted independently, and no wearable device manufacturer had any role in the study design, data collection, analysis, interpretation, or manuscript preparation.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41746-025-01757-1.

Correspondence and requests for materials should be addressed to Cailbhe Doherty.

Reprints and permissions information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.