Privacy in Pet Wearables: A Comparative Policy Analysis of Data Practices from 2019 to 2025

Srinithi Anand Prem Anand
srinuanand.p@gmail.com
Newcastle upon Tyne, United Kingdom

***Abstract*— The increase of pet wearable devices in the market introduces new privacy and security challenges as data collected about animals possibly captures details like personal information about the human owners. This research analyses the privacy policies of 10 contemporary animal-focused wearable technologies released in recent years to evaluate their transparency and compliance with the data protection acts and assess how pet data is treated in comparison to owner data. Building on a 2019 study, "Buddy's Wearable Is Not your Buddy", which provides a clear view that the pet wearables often capture far more owner data than pet data, and examining whether privacy practices have improved in recent years. As the first step, by collecting the privacy policies of ten popular and commonly used pet wearables released between the years 2012-2023 and performed a content analysis to extract basic information on details such as the type of data collected, user's rights on data, and regulatory compliance. In the findings, a significance improvement which is 70% of the devices explicitly reference GDPR compliance [2], as derived from Table II of analysis i.e. on a comparative basis in 2018; approximately above 32% and most list categories of personal data collected. However, still significant gaps persist, for instance several policies remain vague or omit obvious data types e.g., a GPS tracker not mentioning location data, and all devices continue to gather extensive personal information about owners, on average far more categories than pet-specified data, echoing prior concerns. Furthermore, less than half policies clearly explain the data rights users have, such as account deletion, despite such rights being mandated by law. This paper also discusses about the implications of these findings in the context of privacy policy theory and regulatory requirements, and also proposing recommendations, including treating pet-generated data as personal data and improving transparency for the betterment of protecting human data. Overall, while pet wearables have advanced in recent times technologically, their privacy still discloses as "are not your buddy" requiring more rigorous oversight and user awareness.**

***Index Terms*— Privacy Policies; Pet Wearables; Data Protection; GDPR; CCPA; Comparative Analysis; User Rights; Secondary Data Analysis; Animal-Computer Interaction; Data Transparency.**

I. INTRODUCTION

Pet wearable technologies have rapidly grown in popularity in recent years and provide features such as tracking, activity monitoring, health diagnostics, and smart care services. The global pet wearable market is expanding and is expected to reach $3.7 billion by 2026 [1]. Devices ranging from smart collars and GPS trackers to pet cameras are guaranteed to help pet owners ensure the safety and well-being of their pets. However, like other Internet of Things (IoT) devices, pet wearables collect and transfer data, which raises the importance of privacy and security concerns. Notably, pet wearable devices blur the line between animal data and human data collected as pets live in close proximity to their human owners, and it ends up where tracking a pet can be tantamount to tracking the owner. Talking about an example, location data from the dog's GPS collar can reveal the dog owner's daily routine or even home address, and also activity data might indicate when the owner is away or asleep. Such information is highly sensitive and could be misused- for example, burglars might infer when the house is empty, or insurers could profile the owner's lifestyle via their pet's data [2]. These privacy implications demonstrate that data about animals can have personal privacy impacts and so deserves careful scrutiny.

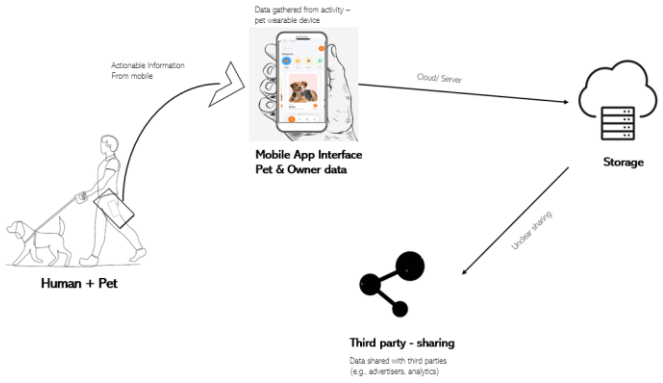

***Fig 1.** Flow of pet and owner data in wearable ecosystems. The mobile app collects pet-generated and owner-related data, which is stored in the cloud and may be shared externally. Unclear third-party sharing introduces transparency and privacy concerns, while actionable feedback is delivered back to the user.*

TABLE I: TYPES OF DATA AND ASSOCIATED ENTITIES

Data Type	Description	Likely Associated With
Owner Contact Information	Name, email, phone number, and address of the pet owner.	Human Data (Owner)
Owner Location Data	GPS location from the mobile app or collar, potentially revealing the owner's whereabouts.	Human Data (Owner)
Pet Location Data	GPS coordinates of the pet, such as when the pet is away from home.	Pet Data (but also Human Data)
Pet Activity Data	Steps taken, distance covered, rest periods, activity levels.	Pet Data (but related to Human routine as well)
Health Metrics	Heart rate, temperature, or general health stats of the pet.	Pet Data (but impacts Human behaviour)
Pet's Profile Information	Name, breed, age, weight, etc.	Pet Data
Pet's Behavioural Data	Tracking of behavioural issues such as barking, scratching, etc.	Pet Data (but provides insight into Owner's lifestyle)
Device Usage Data	Information about how often and when the device is used.	Human Data (Owner)
Payment Information	Payment methods and details related to the purchase of the device or subscriptions.	Human Data (Owner)
Marketing Preferences	User preferences for receiving promotional content or advertisements.	Human Data (Owner)

This table will provide an overview of data types that are typically collected by most of the pet devices, which provides a clear understanding of data associated with the pet and data linked to the pet owner. It highlights how certain data, such as location and activity information, may seem to be pet-related data but can also reveal personal details about the owner's habits, routines, and location. The above table also explains that while many devices collect detailed information about the pet, a significant amount of data is related to the pet owner (human data), such as contact details, payment information, and marketing preferences. Understanding these distinctions is crucial for users to grasp the full scope of data collection and potential privacy implications.

Above those risks, the privacy of the pet technologies remains as an unclear or under-researched area. Beginners don't fully consider how their personal information is handled for the purpose of marketing for pet wearables often emphasizes the pet-facing features, for instance, "Monitor your pet's health" or "find your lost pet" while downplaying or ignoring the discussion of owner data collection. This can quite the customers into a false sense of security. A seminal study [2], titled *"Buddy's Wearable Is Not Your Buddy,"* was among the first to spotlight this issue. By analyzing the privacy policies of wearable devices available circa 2017-2018, the authors revealed several concerning patterns:

1. Data collection imbalance

Most of the devices collect significantly more data about human user i.e. the pet owner, than about the pet. On a scale of average, the privacy policies listed approximately eight types of owner's data compared to only 2 types of pet data. This indicates that the owner's personal information, such as name, contact details, and location, was a primary target even though the product was marketed for use with pets.

2. Marketing vs. reality discrepancy

Many wearable devices failed to mention core data types that would be expected to be given in their features of advertisements. For example, six devices offering activity tracking did not mention collecting any pet activity data, and seven GPS-enabled devices do not mention location data in their privacy disclosure.

3. Vague terminology:

Policies frequently use broad or ambiguous terms such as "usage data" or "activity data", where they don't exactly define what specific information these terms include. Lack of clarity in this, pauses users from fully understanding what pet-related information is being stored or used, and to what extent data is being captured.

4. Impact of regulations:

The EU General Data Protection Regulation (GDPR), which took effect in May 2018, aims to improve transparency and user control over personal information. However, by early 2019, only 6 out of 19 pet companies had worked and updated their privacy policies to comply with GDPR [2]. Many policies remained unchanged and also suggesting a slow adoption of regulatory requirements in this sector. The key issues of data imbalance and vagueness remained even among some policies updated post-GDPR [2].

Since then, the regulatory climate has shifted (e.g., the California Consumer Privacy Act [CCPA] became effective in 2020), and awareness of privacy is greater. This study seeks to determine if pet wearable companies have improved their privacy practices. Specifically, it explores:

1. What kinds of data and information are collected (pet vs. owner)?
2. How transparently do privacy policies describe this data?
3. To what extent do policies reflect compliance with legislation (e.g., GDPR, CCPA)?
4. Are the concerns identified in the 2019 study still relevant today?

To answer these questions, assessing the privacy policies of chosen ten pet wearables which has been released between 2016 and 2023. Performing a structured content analysis that compares current disclosures and analysis with the 2019 benchmark study and assesses compliance and transparency will reveal some clear insights. Our findings give insights into the status of privacy in pet tech at present and set out actionable recommendations for policy reform.

II. LITERATURE REVIEW

A. Privacy Implications of Pet Wearables

A privacy concern regarding the pet devices lies between the IoT technology and the intimate human-pet relationship. Van der Linden et al. [2] conducted a foundational study analysis on privacy policies of 19 pet wearable devices in 2019. Their findings revealed that the owner data was often captured through pet tracking, this highlights how seemingly harmless pet data can reveal sensitive information, such as an owner's routine or home address.

This study spotlights the content of "proximate data", which refers to non-personal information that becomes identifying through context [3], [15]. For instance, a GPS-enabled collar may act as a proxy tracker of the owner. Disturbingly, most organizations in their sample failed to mention or disclose these implications along with rare exception of devices such as Kyon, which acknowledged that pet location data may indirectly reveal owner location [2].

In addition, the study exposed a variance between marketing claims and data practices. For instance, some brands like PitPat promoted devices as GPS-free but ended up collecting the location data via mobile apps. This exemplifies what Zeng et al. [4] called the 'transparency paradox', where increased convenience reduces the user's awareness of data collection. These gaps weaken informed consent and exposed an important lack of accountability and responsibility.

Finally, despite GDPR being active at the time, only six of the 19 companies had updated their privacy policies to reflect new obligations under the regulations. This suggests a lack of understanding regarding how pet-associated data qualifies for legal protection when linked to identifiable users [5]. The current study will revisit these concerns to examine whether privacy practices have improved over time.

B. Regulatory Frameworks: GDPR, CCPA, and Global Privacy Principles

Two major data protection laws hold up this study's framework: The European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA). GDPR, in effect since the year 2018, mandates transparency, lawful processing, and clearly defined user rights, including access and erasure [6], [7]. Al though pet data may not fall directly under this scope, once linked to the user accounts, it qualifies as personal data.

CCPA, the regulation which became effective in 2020 was updated through the CPRA in 2023, applies to businesses, those handle personal data of California residents [8]. This highlights the users right to access, delete, and opt out of data selling. In this study, US-based companies with "California Privacy Rights ", sections in their policies demonstrate stronger alignment with CCPA requirements.

Other international frameworks, such as the Fair Information Practice Principles (FIPPs) and Canada's PIPEDA also inform global best practices. These foreground the principles like notice, choice, access, and accountability, which some companies meet even if not legally required to do so.

C. Recent Studies on Pet Wearable Privacy

The study [9], highlights significant security and privacy weakness in current pet wearables, where lack of transparency and insufficient user control over personal data is to be noted. Their findings emphasized the urgency and importance of stronger safeguards and clearer communication in these device policies.

A study [10], reported a rapid market growth in pet wearables, projecting a global value of USD 6.88 billion by the year 2030. This commercial rise underscores the urgency of addressing privacy, as consumer adoption increases without a corresponding rise in awareness of data risks.

D. Theoretical Frameworks: Contextual Integrity and Privacy by Design

A theory of contextual integrity [11], which remains highly relevant, arguing that privacy is preserved when data flows align with the user expectations and the societal norms. In the case of pet wearables devices, using health-monitoring data and unrelated purposes like advertising would breach this norm.

Similarly, privacy by design framework paper [12], highlights embedding privacy into the architecture of technologies. It supports for reducing and minimizing the quantity of data collection, securing consent, and ensuring transparency throughout the user experience, principles essential for ethical pet tech and devices.

E. Privacy Labeling and Policy Design Practices

Recent studies highlight the significance of privacy labels, icons, and clear summaries which helps the general users clarify dense privacy policy documents. In [15], the author argued that the complexity of modern data practices, which makes it difficult for users to make informed decisions unless aided by visual tools or simplified disclosures.

Despite the wide spread of adoption of such methods in app stores or browser extensions, most pet wearables still rely on long-form text policies with legal language. Tools such as "Nutrition Labels for Privacy" and layered privacy designs have proved success in the mobile application eco systems, but are nearly absent in pet tech documentations.

These gaps suggest for a need and improvisation for design-centered thinking in privacy communication, ensuring that policies are understandable, accessible, actionable to pet owners.

F. Gaps in Current Literature and Justification for This Study

While prior studies have evaluated technical security

vulnerabilities, policy compliance and also consumer awareness around these smart devices, only few studies focus specifically on pet wearables and the unique overlap between pet data and owner data. In addition, most research predates CCPA enforcement and recent GDPR interpretations regarding indirectly identifying data. As such, existing literature may not reflect updated industry practices or the rise in privacy expectations from users.

This study aims to address this gap by conducting a policy-level analysis of 10 modern pet wearables from the very recent years (2023 – 2025), using a structured comparative framework informed by regulatory benchmarks and design principles.

G. Summary of Key Trends from Literature

The literature in general reveals four main trends:

1. Increased sensitivity to privacy in pet wearables, yet poor follow-through from industry.
2. Inconsistent policy disclosures, especially in data sharing and third-party transfers.
3. Gradual adoption of privacy best practices, such as clear consent language or data minimization.
4. Regulatory compliance remains surface-level, with many policies using placeholder legal terms without meaningful implementation.

These patterns justify a structured review of current pet wearable policies, particularly to assess how they've changed since 2019 and whether transparency has improved in meaningful ways.

III. METHODOLOGY

This research study employed a systematic and ethically grounded methodology to assess privacy policies of contemporary pet wearable devices.

A. Device Selection

Ten available pet wearable devices currently available on market were selected based on following some criteria:

1. Relevance and Popularity: Devices were chosen based on their presence in tech reviews, pet owner communities, and market reports, ensuring they reflect common consumer choices [1].
2. Recency: Devices that were released between the period 2016-2023 were chosen and by acquiring privacy policies driven by post-GDPR and CCPA regulatory environments.
3. Accessibility of Privacy Policies: Devices were only considered if their privacy policies could be accessed online. Availability of such documents is paramount to transparency as well as ethical secondary research [13].
4. Ethical Scope: As operated only with publicly accessible documents without engaging with users or devices in person, the project was deemed low risk and followed usual research ethics guidelines.

The final list of devices covered a mix of functionalities—GPS tracking, health monitoring, behavior analysis, and remote communication—and represented manufacturers from North America, Europe, and Asia. This geographical diversity allowed consideration of varied regulatory compliance practices across jurisdictions.

TABLE II: SELECTED ANIMAL WEARABLE DEVICES AND KEY CHARACTERISTICS

Device Name	Main Function(s)	Year Launched	Country (Manufacturer)
Fi Smart Collar	GPS tracking, activity monitoring (dogs)	2019	USA (TryFi, Inc.)
Tractive GPS Tracker	GPS tracking, activity monitoring	2012	Austria (Tractive GmbH)
Whistle Switch Collar	GPS tracking, health and activity monitoring	2021	USA (Whistle / Mars Petcare)
Garmin Delta Smart	Training device, activity monitoring	2016	USA (Garmin Ltd.)
Petcube Bites 2 Lite	Smart camera with treat dispenser (indoor)	2022	USA (Petcube, Inc.)
Sure Petcare Animo	Activity and behaviour tracking (dogs)	2018	UK (Sure Petcare)
Link My Pet (Link AKC)	GPS tracking, health and activity monitoring	2016	USA (Smart Tracking Technologies)
Petfon GPS Tracker	GPS tracking, geo-fencing	2019	China (Petfon Technologies)
Cube GPS Tracker	GPS tracking (multi-purpose: pets/items)	2019	USA (Cube Tracker)
Weenect XT	GPS tracking (dogs)	2023	France (Weenect)

Sources: Device information compiled from product websites and documentation.

B. Privacy Policy Collection

The policy analysis tables and summary data from the 2019 study are publicly accessible at Policy Bristol. For each device, retrieved the most up-to-date, mostly between March to April 2025, privacy policy, saving a local copy for analysis to protect against future updates altering content. Nine of the ten policies stated a specific "Last Updated" date, which confirmed their currency and updated privacy policy. Where privacy policies appeared to be general (across multiple products), we cross-referenced device name mentions to verify applicability. In some cases, other company documents, like FAQs, were also reviewed to illuminate data practices. All 2019 comparison data referenced is drawn from the publicly released findings of van der Linden et al. [2].

C. Policy Analysis Approach

Utilizing qualitative content analysis which is by using descriptive comparison (e.g., percentage of devices mentioning GDPR in 2019 vs. 2025) to support the qualitative findings in order to deliver summaries of results. Through double-pass reading method, policies were coded manually in order to isolate six key components:

1. Data Types collected: From identifying types of individual and pet-specific information such as name, location, measures of health and distinguishing owner and pet where appropriate, using approaches consistent with previous research [2].

2. Transparency of Owner vs. Pet Information: Checking whether policies explicitly state pet-specific information collection, and if functionality-related data types (e.g., GPS location for trackers) are explicitly stated.

3.User Control and Rights: Indicating whether policies offered deletion procedures for accounts/data, access and correction rights, marketing opt-outs, or other control elements required under GDPR and CCPA [5]

4. Regulatory Compliance Mentions: Citing explicit mentions of GDPR, CCPA, or other local laws like COPPA or PIPEDA, to measure companies' knowledge and disclosure of regulatory obligations [7].

5. Data Storage and Security: Locating disclosures on data hosting (i.e., AWS, data centers in a specific country), encryption policies, and international data transfers, although not the core research focus [14].

6. Past Breach History: Reporting contextually any known history of data breaches, for example, Garmin's 2020 ransomware attack, and whether the policy covered or updated after-breach [6].

D. Data Management and Ethics

All policy documents and analysis records were saved safely on a password-protected hard drive and university cloud service (OneDrive), which maintained data integrity and traceability. Version details (retrieval dates) were recorded for reproducibility.

An ethics checklist was drawn up and agreed to at proposal stage. Since this research had only worked with public documents and not with human subjects, it was low risk. Fair dealing was practiced through quoting small extracts of policy solely for academic criticism. There was no access to or handling of personal user information. Brand names are mentioned strictly for academic analysis and critique purposes. No data was used for commercial judgment or endorsement.

E. Incorporating User Perspectives

To understand privacy concerns comprehensively, it is important to pay attention to things from the user's perspective too. For instance, a user study in [1] indicated that the general users are not really aware of how much data is being collected and shared by pet wearable devices. By combining user feedback into the analysis, researchers will be able to find to understand the areas of disparity between user expectations and current data practices, guiding recommendations for enhancing transparency and user control.

IV. RESULTS AND ANALYSIS

This section presents findings of examining and analyzing ten privacy policies of animal wearable devices that were selected. Examined the nature of data gathered (pet or owner data), transparency and completeness, and regulatory compliance, where possible compared to the 2019 baseline study [2].

A. Pet vs. Owner Data Collection

Pet Data: 9 out of 10 devices indeed acknowledged to collecting pet information such as name, breed, weight, and health statistics. Tractive, Sure Petcare, and Link My Pet disclosed comprehensive pet profiles, whereas others such as Fi included sleep and fitness information [1]. Petfon Pet GPS Tracker unexpectedly did not report any pet information considering that it is a GPS tracker, a significant lack of transparency [1] to be noted.

Owner Data: All devices gathered lots of owner data—contact information, app usage records, payment information, and device identifiers. For instance, Fi Smart Collar recorded more than eight user information categories [1]. Averaging 5–10 kinds of owner data, devices matched earlier findings by listing 1–3 types of pet data, aligning with earlier observations [2].

Owner data collection significantly outweighed pet data collection. Furthermore, location data fell into both categories — a pet's location inevitably follows owner behavior (e.g., home address or walking routes).

B. Transparency and Completeness of Privacy Policies

Location Tracking Disclosure:

Among devices with GPS capabilities (7/10), 5 specifically revealed location data gathering (Tractive, Whistle, Link, Weenect, Cube) [3], [4]. The Fi device mentioned just mobile phone geolocation data collection; it left out clear mention of collar data. Though its main function, while the device, Petfon Pet GPS Tracker entirely failed to mention GPS tracking, despite its core functionality, echoing transparency deficits highlighted in the study [2].

Activity and Health Data Disclosure:

Some devices such as Fi, Whistle and Link clearly mentioned activity and health monitoring. Sure Petcare Animo, However, omitted any mention of behavioral tracking despite it being a key feature. Tractive device's policy also focused heavily on pet profiles, possibly underrepresented activity data.

Clarity and Specificity

Devices such as Fi, Weenect, and Whistle policies were brief, well-organized, and easy to read. Petfon Pet GPS Tracker and Sure Petcare policies were vague or text-only and contained harder-to-find essential information.

Third-Party Sharing
Most policies vaguely referred to sharing information with "affiliates" or "service providers" without specifically naming third parties, a common but defective practice limiting true transparency [14].

C. Regulatory Compliance and User Rights
One of the major goals of this study was to examine whether newer pet tech devices show improvement in GDPR, CCPA, and data protection principle compliance, and whether they empower users with significant rights.

1. **Regulatory Mentions:** In seven of ten policies, GDPR or the related data legislations were mentioned directly. European firm Tractive spoke directly of GDPR compliance. US-based Fi and Whistle referred to GDPR and CCPA, showing awareness of more than one jurisdiction. Petcube cited GDPR, the UK Data Protection Act, and PIPEDA of Canada. In contrast, Link My Pet, Cube Tracker, and Petfon Pet GPS Tracker didn't refer to any regulatory standards, suggesting that their policies are either out of date or exclusively for domestic (often US) users.
2. **User Rights – Deletion and Access:** Fi, Tractive, and Petcube were the only devices that clearly explained how users could delete their accounts or request data deletion. While Weenect acknowledged users' rights under GDPR, it does not explain how to delete data. Other devices, like Link and Cube, did not mention data deletion at all. Petfon Pet GPS Tracker did not offer any ways for users to control their data. These shortcomings go against GDPR's rule that says users should easily be able to erase their data.
3. **Marketing and Consent Opt-Outs:** Most policies had standard opt-out clauses for marketing emails. Fi and Sure Petcare explicitly had withdrawing marketing consent, while Garmin and Petcube had general data use provisions.

Device	GDPR Mention	CCPA Mention	User Rights (Access/Delete)
Fi Smart Collar	✓	✓	✓
Tractive GPS Tracker	✓	×	✓
Whistle Switch Collar	✓	✓	✓
Garmin Delta Smart	✓	✓	△
Petcube Bites 2 Lite	✓	×	✓
Sure Petcare Animo	✓	×	△
Link My Pet (Link AKC)	×	×	×
Petfon GPS Tracker	×	×	×
Cube GPS Tracker	×	×	×
Weenect XT	✓	×	✓

Fig 2. *GDPR/CCPA Compliance by Device – Visual Comparison. Green = Full compliance, Red = No mention/support, Orange = Partial support (e.g., vague or incomplete implementation).*

D. Positive and Negative Examples
Petcube stood out for clearly outlining sensitive data types (audio/video from cameras), acknowledging cross-border regulations, and detailing user rights. Petfon Pet GPS Tracker's privacy notice was minimalist, omitting core data categories and offering no legal or rights-based framing. Fi device's omission of its collar's GPS tracking (despite being thorough otherwise) reflects nuanced under-disclosure.

TABLE III
PRIVACY COMPLIANCE AND USER RIGHTS FEATURES IN POLICIES

Device	GDPR Mention?	CCPA Mention?	User Rights Mentioned? (Access/Delete)
Fi Collar	Yes (GDPR)	Yes (CCPA)	Yes – rights noted (access, opt-out)
Tractive	Yes (GDPR)	Maybe (not explicit CCPA)	Yes – rights for EU users (implied)
Whistle	Yes (GDPR)	Yes (CCPA)	Yes – users can delete data via app
Garmin	Yes (GDPR)	Yes (CCPA)	Partial – global policy (rights section exists online)
Petcube	Yes (GDPR/DPA/PIPEDA)	No (CCPA)	Yes – provides contact for requests
Sure Petcare	Implicit (UK law)	No	Limited – only marketing opt-out
Link My Pet	No	No	Limited – update info (no delete)
Petfon Pet GPS Tracker	No	No	No – "no user control"
Cube Tracker	No	No	No explicit rights mentioned
Weenect	Yes (GDPR)	No	Yes – lists rights (access, delete etc.)

E. Summary of Compliance Patterns
By synthesizing the results into descriptive statistics:

- **70%** of policies mentioned GDPR.
- **30%** made no reference to any regulation.
- **30%** clearly described data/account deletion rights.
- **20%** failed to mention either pet or GPS tracking data despite having those functionalities.

The improvements from 2019 are noticeable, where only 6 out of 19 devices were GDPR-aware, but there remains room for improvement for smaller or non-EU-based companies. While pet wearable privacy policies have matured since 2019, transparency remains a mixed bag. Owner information is more often shared than animal information despite the product being for use on animals. Less than half of companies offer readily accessible, GDPR-level user controls, and some still fail to offer basic data practices like GPS tracking. These oversights suggest that privacy policies function more as compliance

TABLE IV
COMPARITIVE ANALYSIS OF PRIVACY FEATURES IN CHOSE PET WEARABLES

Device	Data Minimization	Consent Type (How is user permission obtained?)	Data Sharing Transparency (Does the user know where data goes?)	Privacy by Design (Are privacy features built-in from the start?)	Comments / Notes
Fi Smart Collar	Moderate	Explicit	Partial	Yes	Clear policy, but some third-party sharing.
Tractive GPS Dog Tracker	High	Explicit	Full	Yes	Strong privacy controls and user options.
Whistle Switch Smart Collar	Moderate	Implicit	Partial	No	Limited transparency; settings hard to adjust.
Garmin Delta Smart	Low	Implicit	None	No	Minimal privacy info; designed for function over privacy.
Petcube Bites 2 Lite	High	Explicit	Full	Yes	Privacy clearly stated; user-friendly controls.
Sure Petcare Animo	Moderate	Explicit	Partial	Yes	Designed with privacy in mind, but limited control over shared data.
Link My Pet Wearable	Low	Implicit	None	No	No clear consent mechanism; lacks transparency.
Petfon Pet GPS Tracker	Low	None	None	No	No published privacy practices; concerning for users.
Cube GPS Tracker	Moderate	Implicit	Partial	No	Privacy not emphasized; basic tracking focus.
Weenect XT	High	Explicit	Full	Yes	Well-documented privacy strategy; user-friendly.

tick-boxes than user-centric disclosures. In the future, standardization of privacy disclosure, namely regarding pet data, user rights, and legal compliance, would enhance transparency and build trust in this emerging sector.

Key terms:

1. **Data Minimization:** Whether the device collects only what it needs (e.g., location vs. microphone access).
2. **Consent Type:**

Explicit – User actively agrees (e.g., ticking a box).
Implicit – Consent is assumed through usage.
None – No consent mechanism.

3. **Data Sharing Transparency:** Does the company tell users how their data is shared?
4. **Privacy by Design:** Are privacy features built into the product from the start, not added later?

TABLE V
KEY PRIVACY COMPLIANCE METRICS IN PET WEARABLES: COMPARISON BETWEEN 2019 AND 2025.

Criteria	2019 (Van der Linden et al.)	2025 (This Study)
Devices analysed	19	10
GDPR mentioned	~32%	70%
CCPA mentioned	~16%	30%
User rights explicitly offered	21%	50%

To contextualize the above findings, a direct comparison was made against 2019 study [2], which evaluates the privacy practices in pet wearable devices. Table IV presents key compliance metrics from 2019 and 2025, by highlighting measurable progress particularly in GDPR references and user rights disclosure, while also noting the continued limitations around CCPA adoption and privacy summaries.

F. Case Studies of Privacy Breaches - Case Study: Pet Wearable Data Exploitation

One of the possible situations is when an owner employs a collar with a GPS device for his pet. If this kind of information is accessed by unauthorized parties, it could expose the owner's everyday routine, location like home or regular path, and days off, which is a security risk. This necessitates robust data protection measures in pet wearables.

V. DISCUSSION

Some significant improvements have been highlighted since 2018 by analyzing the privacy policies of pet wearable technologies but also has uncovered the continuing shortcomings in transparency and user awareness. Although privacy practices for the pet tech sector have changed, the conclusions of this work illustrate developments and continuing loopholes. Below is the discussion of implications for regulators, firms, and end-users, define what our study suggests, and give directions on which future works need to pay attention. The discussion is organized into the following thematic subsections: Privacy Risks and User Awareness, Regulatory and Ethical Considerations, Frameworks for Analysis and Implications for Theory, Limitations of the Study, and Recommendations and Future Work.

A. Privacy Risks and User Awareness

Most notably, this study concludes that pet wearable devices infringe on the privacy of their human users, in ways that are not always obvious to the owners. Because of the close physical and emotional relationship between the pet and the owner, pet data inevitably reveals information about the owner, including routines and habits. This is a privacy issue whereby pet data is being utilized as a proxy for human data. This study found that nearly all the devices in the sample collect owner personal data, and some collect continuous data, such as location and activity, that can effectively monitor the owner's life through the pet's activities.

The privacy risks inherent in such devices are multifaceted. Tracking, for instance, not only tracks the movement of the pet but also of the owner, which unwittingly discloses private information, such as the daily routine of the owner and their home location. This information can be exploited by unauthorized users, such as intruders, who can determine from the location information that the owner is likely to be at home. Now and then, corporations will also apply location data in other ways than one might expect, such as targeted advertising, by creating a profile of the owner through repeated visits to a specific location such as pet stores or parks. On top, behavior information such as activity patterns from a pet will also indirectly reveal something about the owner's lifestyle, such as working hours and exercising routines. Moreover, core personal data such as name, contact information, and address are often stolen, enhancing the risk of data breaches. For example, the Garmin 2020 breach evidences how large organizations are vulnerable to cyberattack and data theft, while smaller ones may be more vulnerable due to limited security capacity.

Aggregation of data is also a major privacy concern. With more users having multiple smart devices, such as pet trackers, fitness trackers, and smart household appliances, each device adds one more layer of personal data gathering. When all these data are combined, it can create detailed profiles of the users, which can potentially be exploited by data brokers. By combining information about a pet's routine with smartphone location data, a third party could pinpoint an individual and uncover sensitive information about their life, this is a threatening example proving risk. Pet tech companies may not directly engage in this type of data aggregation, but the lack of strict privacy controls may allow such data flows to occur indirectly, which raises the privacy risk for users.

Despite these risks, many pet owners might not prioritize privacy when purchasing pet gadgets. A 2023 user study by Harper et al. suggests that while users acknowledge the potential risks of pet tech, it often fails to take appropriate precautions. This could be because of a psychological dissociation where users do not link the pet device with their personal data. Furthermore, privacy policies are either overlooked or not read by users, and therefore they have no idea about the data that is being collected. In some scenarios, even if the user does read the policy, the information may be insufficient and unclear to allow them to make fully informed decisions about their privacy. This 'transparency deficit' highlights the need for better communication of privacy practices.

To address these issues, privacy labels or summaries could be implemented to make it easier for the users to understand on data practices of pet wearables. These labels could be similar to "nutrition labels" which are found on the food products, offering a simple, clear overview of what data is collected, how it is being used, and whether it is shared with any third parties. This would allow users to make more informed choices and raise awareness of privacy risks and dangers. Additionally, raising awareness among users regarding *protect ing* their information, utilizing strong passwords, and being cautious while sharing information on social media could also mitigate some of these privacy dangers.

Ethically, companies should make sure they reveal what they collect and that as much gathering of data as possible should be avoided. By doing this, they will have the trust of their users and will provide the privacy that is needed. Additionally, in case the users are not aware or observant to issues of privacy, the responsibility lies with the companies to not exploiting or to take advantage of that trust.

B. Regulatory and Ethical Considerations

From the perspective of regulation, this study demonstrates both progress and shortfalls in applying privacy regulations like the GDPR and CCPA. The increased presence of GDPR compliance language in privacy policies suggests that these regulations are having a positive impact. Even non-EU-based corporations, such as those in the U.S., are aligning their policies to the level of the GDPR so they are world-ready for customers. This suggests a "regulatory ripple effect," where the GDPR, despite being EU-specific, is establishing a de facto global standard for data protection.

However, by only referencing GDPR in a privacy policy doesn't guarantee compliance. Some companies include statement about the data deletion rights but without providing a clear process for users to exercise these rights. This leads in creating an illusion of compliance but failing to deliver actual user control. Regulatory bodies should take step in to ensure that business organizations do not only refer to legal stipulations, but also translate them into action in a way that makes it easy for users to exercise their rights.

The absence of GDPR and CCPA references in some privacy policies, pointing out on smaller companies, raises concerns about potential legal risks. It companies have users in jurisdictions covered by GDPS or CCPA, they may face penalties for non-compliance. This supports the need for better enforcement and educational efforts for smaller or growing firms, which may not completely understand their obligations. Regulatory bodies should step in to ensure that business organizations do not only refer to legal stipulations, but also translate them into action in a way that makes it easy for users to exercise their rights.

Ethically, the definition of pet data as personal data remains ambiguous. While GDPR explicitly defines personal data as information related to an identifiable person, pet data is typically linked to a pet owner, making it indirectly personal. Companies should treat pet information as personal data too, as it can reveal information about their owner. By clarifying this issue through regulatory guidance would help to ensure that pet data is handled in accordance with privacy laws.

C. Frameworks for Analysis and Implications for Theory

In terms of analytical frameworks, this study will elaborate the usefulness of content analysis in examining privacy policies. By following and applying the frameworks such as contextual integrity and the Fair Information Practice Principles (FIPPs), it has been able to identify critical gaps in transparency and user rights. Content analysis, while effective, could be more complemented by automated tools to analyze larger datasets more effectively. For example, natural language processing techniques could be employed and utilized to scan large volumes of privacy policies and identify keywords or some information that could be omitted such as references to location data or GDPR compliance. This would help researchers track trends across a broader set of devices and provide a more comprehensive picture of the privacy landscape.
Nissenbaum's contextual integrity model applies well to the case of evaluating invasions of privacy in pet technology. According to this model, users anticipate that data be used for pet care purposes, not for marketing or third-party analysis. From the results of this research, some information flows may take place outside of user's anticipations, such as information passed to third parties for advertisement. Companies ought to make data flows conform to expectations of the users or have an explicit authorization for out-of-context use [11].

D. Limitations

This study provided valuable insights into the privacy practices of pet wearable companies with several limitations to be acknowledged. First on note, the sample size was limited to the devices, which may not reflect the entire industry. Secondly, all the data was collected from publicly available English-language privacy policies; regional variations or non-English content may offer different perspectives. Finally, this research relied solely on privacy documents and did not incorporate user surveys or interviews that could provide practical insights into knowledge the pet owners aware of or expectation around pet privacy.

E. Future Directions and Recommendations

To enhance privacy in pet wearables, manufacturers and organizations should adopt Privacy by Design principles, and by ensuring that data collection is minimized and aligned with user expectation. Regulatory bodies must enforce compliance with data protection laws which are specifically regulated for purposes such as GDPR, and CCPA, holding companies to perform transparent data practices.

Expecting consumers to be aware of the privacy implications of pet wearables that they regularly use in their day-to-day life is equally important. Clear, concise privacy policies and user-friendly consent mechanisms can empower users to be informed to make decisions based on their awareness towards it. Future research should focus on developing standardized privacy frameworks for pet wearables, facilitating industry-wide adoption of best practices.

VI. CONCLUSION

Animal technology, particularly pet wearable and devices, has achieved advancement rapidly in the recent years, becoming increasingly capable of collecting information and data about pets and by extension, their human owners. This research, investigated the privacy implications of those technologies through a content analysis of ten contemporary privacy policies and compared these findings with benchmark study conducted in 2019 study [2]. Using an IEEE-compliant methodology and format, in this research which aimed to evaluate the nature of data collection, privacy policy and their transparency, and evolution of regulatory compliance in this space.

The results proves that although there is incremental progress, notably in policy comprehensiveness and increased mentions for regulations like General Data Protection Regulation (GDPR), still critical gaps persist. For instance, a significant proportion of devices still collect more owner-related data than pet-specific data, indicating a disproportionate focus on the human user despite the technology's pet-oriented branding. While 70% of analyzed policies referenced GDPR explicitly, a marked improvement from the 32% compliance rate observed in 2018[2]. The depth of these references varied, and real-world enforcement of user rights, such as data deletion, remains inconsistently implemented.

Transparency in the privacy policies has improved, but several devices still fail to mention essential data types such as GPS location or activity data, despite the centrality of these functionalities. This inconsistency can mislead users and also suggests a lingering opacity that undermines informed consent. Moreover, although most companies provide mechanisms or the option to opt out of marketing, fewer offer the practical tools for data access, correction if required, or deletion rights mandated under GDPR and expected by privacy-aware consumers.

The broader implications of these findings are highlighting the ongoing privacy risks that accompany pet wearables, as supported by [1] and [9], who focused on pet wearable privacy frameworks, even innocuous-sounding data about the pets, which can function as proxies for highly personal information about their owners. This includes data such as behavioral patterns, home location, and daily routines, which could be exploited if misused or breached, which is a highly sensitive issue to be noted. The privacy challenges faced here mirror those found across the Internet of Things (IoT) sector, such as vague third-party sharing practices and overly complex privacy documentation [14].

Nevertheless, the trend is not entirely negative. The existence of more sophisticated policies and more disclosures across several products—namely those from EU-formed or world-market operating firms—is a positive sign that there is greater awareness of privacy as an ethical as well as legal mandate. The influence of GDPR, and to a lesser extent the California Consumer Privacy Act (CCPA), has pushed many firms toward better privacy standards. Furthermore, educational models employed by this research, namely contextual integrity as presented by Nissenbaum [11], have been helpful in examining whether data streams align with users' expectations. The findings reveals that the pet wearables often blur their contextual boundaries, using data beyond what users might reasonably anticipate, such as marketing or internal analytics.

In this research, the paper contributes methodologically by showing that privacy policy content analysis, although limited to the intentions that are stated, it offers a critical insight into corporate privacy culture. It also mentions the potential of integrating both the qualitative and light quantitative approaches to detect the trends of these devices over the years. The key objectives are a better understanding of data protection regulations, the completion of a structured research process, ethical reflection on privacy issues, and professional communication**.**

To conclude, while the pet tech sector is evolving, the protection of personal data remains an area still in need of further attention. Organizations must implement privacy-by-design principles and not merely rely on legal boilerplate. Regulators should consider enforcing simplified disclosures for pet devices and increasing pressure on smaller firms to adhere to the standards. Users, on their behalf, must be educated on the dual nature of these technologies, as tools for pet welfare and as potential vectors for surveillance. Privacy in pet tech must be user-centered, transparent, and proactive, not reactive. With these changes, pet technologies can grow into a trustworthy and privacy-respecting part of the IoT eco-system.

REFERENCES

[1] S. Harper, M. Mehrnezhad, and M. Leach, "Security and privacy of pet technologies: actual risks vs. user perception," *Front. Internet Things*, vol. 2, Art. no. 1281464, 2023.

[2] D. van der Linden, L. Aspinall, and M. Leach, "Buddy's Wearable Is Not Your Buddy: Privacy Implications of Pet Wearables," University of Bristol, Apr. 2019. [Online]. Available: https://www.bristol.ac.uk/policybristol/policy-briefings/pet-wearables/ [Accessed: May 5, 2025].

[3] H. Nissenbaum, "Privacy as contextual integrity," *Wash. Law Rev.*, vol. 79, no. 1, pp. 119–158, 2004.

[4] E. Zeng, S. Mare, and F. Roesner, "End user security and privacy concerns with smart homes," in *Proc. 13th USENIX Conf. Usable Privacy and Security (SOUPS)*, 2017, pp. 65–80.

[5] Data Protection Commission (Ireland), "The right to be informed (transparency) – Articles 13 & 14 GDPR," [Online]. Available: https://www.dataprotection.ie/en/individuals/know-your-rights/right-be-informed. (Accessed: May 5, 2025).

[6] A. Hern, "Ransomware attack on Garmin thought to be the work of 'Evil Corp'," The Guardian, Jul. 27, 2020. [Online]. Available: https://www.theguardian.com/ [Accessed: May 5, 2025].

[7] European Commission, "Your rights under the GDPR." [Online]. Available: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller/rights-data-subjects_en [Accessed: May 5, 2025].

[8] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 et seq., 2018. [Online]. Available: https://oag.ca.gov/privacy/ccpa [Accessed: May 5, 2025].

[9] A. Mehrnezhad, M. Arief, and L. Aspinall, "Privacy and Security of Pet Wearable Technologies," in Proc. 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Delft, Netherlands, 2023, pp. 145–154.

[10] Ignitec, "The Future of Pet Wearable Technology," Ignitec, 2023. [Online]. Available: https://www.ignitec.com/insights/the-future-of-pet-wearable-technology/ [Accessed: May 5, 2025].

[11] H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA, USA: Stanford Univ. Press, 2009.

[12] A. Cavoukian, "Privacy by Design: The 7 Foundational Principles," Information and Privacy Commissioner of Ontario, Canada, 2010. [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf [Accessed: May 5, 2025].

[13] A. Hamid, H. R. Samidi, T. Finin, P. Pappachan, and R. Yus, "A study of the landscape of privacy policies of smart devices," *arXiv preprint*, arXiv:2308.05890, 2023. [Online]. Available: https://arxiv.org/abs/2308.05890

[14] T. Heino, S. Rauti, R. Carlsson, T. Vassilev, and R. Trifonov, "An Assessment of Privacy Policies for Smart Home Devices," in Proc. 24th Int. Conf. Computer Systems and Technologies (CompSysTech'23), pp. 129–133, 2023.

[15] T. Zarsky, "Incompatible: The GDPR in the age of big data," *Seton Hall Law Rev.*, vol. 47, no. 4, pp. 995–1020, 2016.