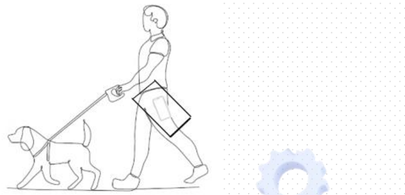
Privacy in Pet Wearables: A Comparative Policy Analysis of Data Practices from 2019 to 2025

Srinithi Anand Prem Anand
Department of Advanced Computer Science
Northumbria University

This study reviews privacy policies of 10 pet wearables, focusing on owner vs. pet data collection, transparency, and GDPR/CCPA compliance. While 70% referenced GDPR, most lacked clear user rights disclosures and over-collected owner data. Compared to the 2019 benchmark, progress is visible — but major gaps in policy clarity and ethical data handling remain.

DO PET DEVICES SERVE PETS, OR ARE THEY QUIETLY COLLECTING PERSONAL DATA ABOUT OWNERS?

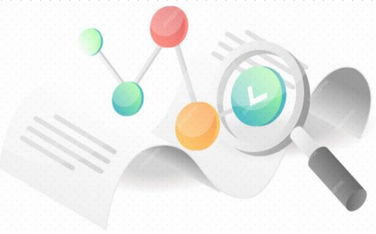


Research Motivation & Problem

As pet wearables become increasingly common, privacy risks grow due to the close relationship between pets and owners. Pet data, like location or behavior, can inadvertently reveal sensitive information about the owner. Many policies downplay this by focusing only on pet features, ignoring the human privacy impact. This study addresses the overlooked problem of how these devices treat owner-related data under the guise of pet care, identifying a significant knowledge and regulatory gap.

Existing Approaches

Previous research (notably van der Linden et al., 2019) revealed that pet wearables collected much more data about owners than pets, while privacy policies lacked detail or omitted obvious functionalities. Many devices didn't even mention GPS tracking or behavioral monitoring despite advertising such features. While GDPR came into effect in 2018, only a small number of companies updated their policies accordingly. This research revisits those same themes to check whether the situation has improved in the current privacy climate.



Research Approach

The privacy policies of 10 pet wearable devices, were analyzed using a comparative framework. Each policy was evaluated across six dimensions:

1. Types of data collected (owner vs. pet)
2. Clarity and specificity of disclosures
3. User rights (e.g., account/data deletion)
4. Legal references (GDPR, CCPA)
5. Security disclosures and third-party sharing
6. History of data breaches or public trust issues

Methodology

- **Device Selection:** 10 pet wearables selected for popularity, feature diversity, and policy accessibility.
- **Data Collection:** Policies retrieved between March and April 2025.
- **Analysis Method:** Qualitative content analysis using double-pass manual coding.
- **Frameworks Used:** Contextual Integrity, Privacy by Design, and legal benchmarks from GDPR and CCPA.
- **Ethics:** No human data used; only public documents analyzed.

Key Contributions

- Assessed post-GDPR/CCPA privacy in pet wearables
- Found owner data > pet data in all cases
- Defined pet data as indirectly personal
- Suggested clear, user-friendly policy design

Challenges

- ✓ Vague terminology like "usage data" hides real data collection.
- ✓ Policies do not match advertised features (e.g., GPS not mentioned).
- ✓ Inconsistent compliance with GDPR/CCPA.

Solutions

- ✓ Use privacy labels for simplified policy summaries.
- ✓ Improve UI for consent and data deletion.
- ✓ Mandate clear legal disclosures and third-party data use statements.

Results

- ❖ Regulatory Acknowledgment: 30% of policies made no mention of any legal frameworks, reflecting ongoing inconsistency in industry compliance.
- ❖ User Rights Transparency: Only 3 out of 10 devices (30%) clearly outlined user rights related to data deletion or account termination, despite these being fundamental requirements under GDPR and CCPA.
- ❖ Data Collection Disparity: Every device in the sample collected significantly more owner-related data than pet-specific data.
- ❖ Location Tracking Disclosure: Several GPS-enabled devices failed to explicitly disclose location data collection in their policies, despite marketing GPS as a core feature.
- ❖ Policy Quality Spectrum: Some devices lacked fundamental disclosures, failing to meet even basic standards for transparency or user control.

Future Work

- Expand analysis to upcoming pet devices (2025+).
- Include user interviews to assess privacy awareness.
- Explore basic automation for policy text comparison.
- Draft a sample privacy label for pet tech policies.

Conclusion

Privacy policies have improved, but transparency and user control remain limited. Owner data continues to dominate, while legal compliance varies. Clearer disclosures and ethical handling of pet-related data are essential to protect both pets and owners.