

Privacy implications of pet wearables

**Dr. Dirk van der Linden, Dr. Barney Craggs, Prof. Awais Rashid (University of Bristol, UK)
Dr. Anna Zamansky, Dr. Irit Hadar (University of Haifa, Israel)**

Pet wearables have significant privacy implications for consumers. This research into the extent of data collected by pet wearables has led to a clear understanding that consumer pet wearables available on the market capture far more data of owners than actual pets, and potentially mislead consumers into underestimating this extent of data capture. Moreover, pet data descriptions are often vague and may understate their potential to indirectly identify their owners or third parties.

About the research

The billion-dollar pet industry is catching up on the wearables hype and getting involved in the wearables market – producing activity trackers, location trackers, and advanced health and sleep wearables to allow pet owners more insight into their beloved pets.

However, pet wearables are marketed to consumers focusing heavily on the pet as the user of the device, while making little mention of whether, and to what extent, owners will have to give up their personal data as well to use the accompanying software. Consumer's desire to provide the best care for their pets combined with such marketing may lull them into a false sense of security by understating that they are the actual user of the product, and subsequently likely tracked as such.

Moreover, tracking the activity or location of pets is equally as sensitive as tracking users directly, as pets are typically around us. Access to pet activity data could be used to build profiles on pet owners, with implications ranging from burglars knowing when to approach a home, to insurance companies inferring health profiles of pet owners via their dog's activity.

This collaborative research between British and Israeli universities has provided clear insights into the extent of data known to be captured by 19 pet wearable devices available to consumers.



Policy recommendations

Consider explicitly marking pet activity data as personal data

- Similar to activity data from personal trackers, activity data from pets co-located with humans should be marked as personal data, capable of identifying them, and treated with relevant protection (encryption, deletion requests, etc.)

Consider requiring clear marketing based on whose data is captured

- While pets may physically wear the devices, over-emphasizing them as the “user” or “wearer” of these devices understates the extent of data captured by software used to interact with the device.

Consider enforcing FAQ answers based on not only the physical device but connected devices too

- If a pet wearable states that it does not contain GPS and does not track the pet's location, consumers will likely understand this to mean no location is tracked. Yet, sensors in connected devices (such as the owner's smartphone) are often still used to track location.

Policy analysis: what data is known to be captured?

We extracted the data mentioned by each device’s privacy policy, integrating trivial synonyms like “log in” and “login”. Where comparing data was not trivial such as “activity data” and “exercise data”, we left data separate. We only considered data collected by the service/devices themselves, not any data collected by third parties via e.g., Facebook.

We analysed privacy policies at two distinct moments: December 2017, before the GDPR was in effect, and June 2018, after the GDPR came into effect. We specifically noted any additional data mentioned in updated policies and changes, if any, spurred by the GDPR.

Key findings:

- Several devices have critical mismatches in marketing and their key data: 6 devices with activity tracking functionality did not detail any pet activity data in their privacy policies, while 7 devices with location tracking functionality did not detail any location data in their privacy policy.
- Most devices capture more owner data (average 8 items) than pet data (2 items)
- The GDPR has not had a significant effect in this sector, as only 6 out of 19 devices have updated their policies to be compliant with new legislation since the GDPR came into effect. Yet, the key findings above still apply to them.
- It is unclear what pet data is stored (and inferred) by use of ambiguous terminology such as “activity data”.

Number of data items known to be captured for pets and owners:

	FitBark	Garmin DeltaSmart	Jaeger & Lewis	Kippy	Kyon	Link AKC	Nuzzle	Paby	PawTrack	PetPace	PitPat	Poof (bean/pea)	Scollar	TabCat	TractiveGPS	TractiveMOTION	Whistle	WonderWoof	Wüf
number of pet data items captured	3	0	2	0	2	5	0	4	0	4	14	0	0	0	1	1	4	1	3
number of owner data items captured	7	4	3	0	8	17	4	10	5	1	15	3	20	0	9	9	14	12	10

Devices with critical mismatches between marketing and data capture:

	Garmin DeltaSmart	Link AKC	Nuzzle	PawTrack	Poof (bean/pea)	Scollar	TabCat	TractiveGPS	TractiveMOTION	WonderWoof
Activity tracking functionality without detailing whether activity data is stored	?		?		?	?		?	?	
Location tracking functionality without detailing whether location data is stored		?	?	?	?	?	?	?		

Further information

van der Linden, D., Zamansky, A., Hadar, I., Craggs, B., Rashid, A. (2018). Buddy’s wearable is not your buddy – privacy implications of pet wearables. IEEE Security & Privacy, 17(3). 10.1109/MSEC.2018.2888783

