Author advance copy of accepted manuscript. Cite as:

D. van der Linden, A. Zamansky, I. Hadar, B. Craggs, A. Rashid, "Buddy's wearable is not your buddy: privacy implications of pet wearables," in IEEE Security & Privacy, forthcoming, doi 10.1109/MSEC.2018.2888783

Buddy's wearable is not your buddy: privacy implications of pet wearables

Dirk van der Linden[1], Anna Zamansky[2], Irit Hadar[2], Barnaby Craggs[1], and Awais Rashid[1]

[1] Department of Computer Science, University of Bristol, UK
dirk.vanderlinden,barney.craggs,awais.rashid@bristol.ac.uk
[2] Department of Information Systems, University of Haifa, Israel
annazam,hadari@is.haifa.ac.il

Abstract. As an increasingly prevalent class of consumer device, pet wearables hold more privacy implications than might at first be apparent. Whilst marketed as devices for pets, through analysis of privacy policies we show that more data is captured about owners than pets – and what data is captured remains vague.

Keywords: wearable computing, technology social factors, privacy, data privacy, animals, pets

1 Introduction

One might be tempted to have assumed that consumers understand the privacy risk stemming from the use of wearables. Research has shown that wearables are a major source of privacy concern for their users [1], and data leaks are frequently reported in the media. For example, standard (opt-out) tracking functionality enabled on FitBit devices shared into the Strava app was recently confirmed to have led to a leakage of sensitive strategic information [2]. Yet, research has also shown that perceived privacy risk has little correlation to consumers' intention to use wearables, let alone the perceived enjoyment of that use [3].

We focus on a potentially insidious threat to our privacy via a new class of seemingly innocuous wearables: the pet wearable. Pet wearables, like other wearables, consist of two distinct data gathering points: the actual wearable worn by the pet and the related software, typically running on the owners' phone and thus allowing for extensive data collection on the owner. Figure 1 visualizes the key relations here. Unlike other wearables, the way pet wearables are marketed to consumers focuses heavily on the pet-related functionality the device provides (e.g., locating a missing pet, tracking walks) 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. Knowing that consumers are swayed by the rhetoric and perceived benefits of wearables, with little thought offered towards the potential risks of their use [4], the way these devices are marketed is an important factor in their adoption and use. If consumers of pet wearables are typically told, with almost exclusive focus, what the wearable will measure of the pet, and how this information can be used to improve its wellbeing, it may lull consumers into a false sense of security by understating that they are the actual user of the product, and subsequently likely tracked as such.

In this paper, we show the privacy threat originating from pet wearable use by analyzing their privacy policies to assess what data they are (not) known to capture. Our key findings

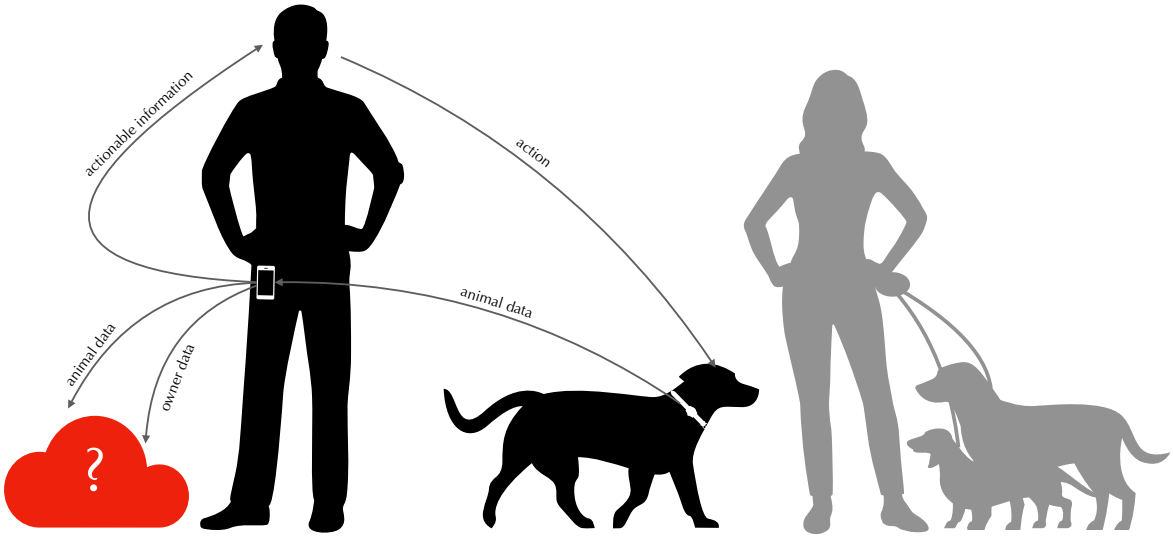

Fig. 1. The context of a typical pet wearable: the wearable sends pet data to an app, which collects additional owner data, and stores both somewhere'. This data is used to generate actionable information for the owner, who then takes actions towards the pet. Pet data may indirectly reflect the pet's immediate surroundings due to its interaction with, or reaction to elements in those surroundings (e.g., third parties, being left home-alone, pet boarders).

include that some pet wearables do not consider the sensitive nature of pet data, are vague in stating exactly what they track, seemingly track far more data of the owner than the pet and that there is indeed a recurring mismatch between how pet wearables are marketed and what data they are known to track. As a result, consumers need an unreasonable degree of alertness to infer the extent of their personal data that may be unexpectedly and indirectly captured.

The rest of this article is structured as follows. Section 2 explores different privacy threats following from pet wearables use. In Section 3 we analyze popular pet wearables currently on the market and the data they are known to capture according to their privacy policy. We discuss the consequences of these findings in Section 4, and further reflect on their implications in Section 5. We conclude with recommendations in Section 6.

2 Pet wearables and privacy threats

The increasing use of pet wearables makes it important to understand what new privacy threats their use brings. Knowing that humans typically co-exist with their pets in a close relationship it is reasonable to assume that capturing data of a pet will reveal information on the owner. Compare, for example, the notion of tracking a phone. In a TED Talk [5] in 2012, Malte Spitz highlighted the extreme extent to which mobile telecommunications companies log, track and utilize the meta-data that underpins this personal device usage. By tracking the user's mobile phone, the service provider was essentially without consent tracking Spitz's (and every other user's) lives and breaching privacy. It is now widely understood that tracking

a mobile phone is tantamount to tracking its users, because of the relationship between the user and the phone. Tracking of pet data, similarly, may reveal a detailed picture of their owners' habits and whereabouts. To complicate matters, an owner in this sense may practically be more than a single person. For example, different family members interacting with their pet, an incidental dog or cat sitter, or even a veterinarian – all may be reflected in the pet's data. Exactly whose personal data the pet data may reveal thus becomes an additional concern.

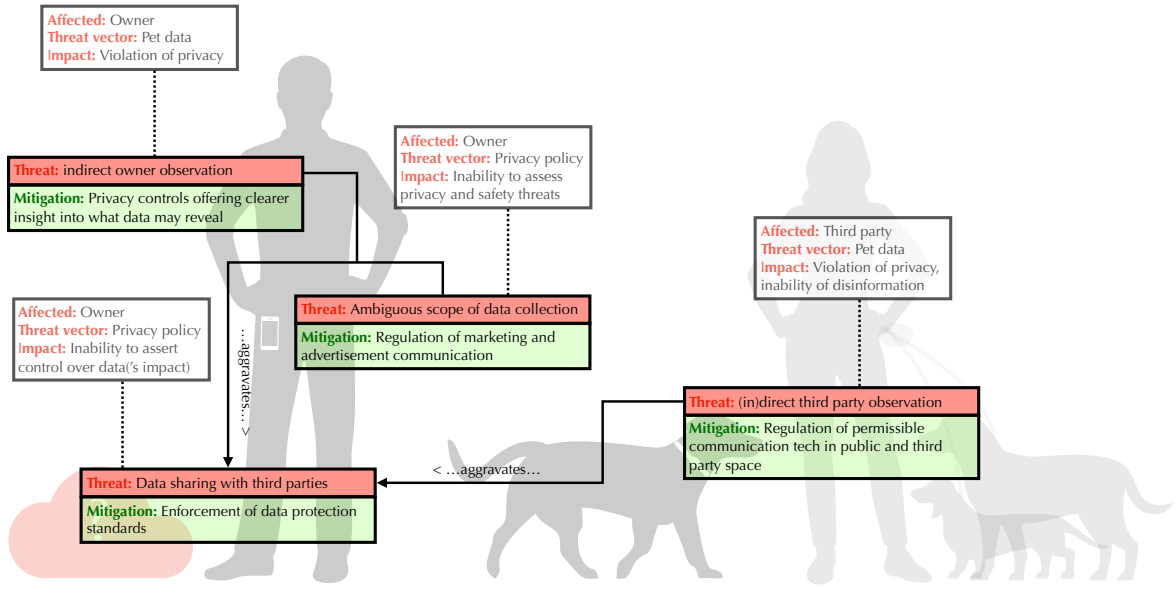

Fig. 2. Data privacy threats of pet wearables: the ambiguous scope of data collection, and (in)direct third party observation allowed by these products aggravate the common threat of data sharing with third parties.

Many pet wearables use accelerometers to capture activity data of pets, which allows for the deduction of complex behavior. Ladha et al. [6] presented a classification system that can deduce sixteen advanced canine behaviors and poses such as shaking, shivering, sniffing, digging – all of which may be in response to outside stimuli. 'Mere' accelerometer data of a dog thus has the opportunity to be classified into a detailed account of physical context a dog was in – out for walks at specific times in the morning and evening, playing in the afternoon, napping at some other times. Such information 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. Pet data itself, thus, may contain very sensitive information with the strong potential for privacy intrusions, allowing for consumer's fear "of certain data, when combined, having critical implications." [1]

This is all the more concerning as research has argued that many datasets captured by wearables cannot be realistically (considered) de-identified or pseudonymised because sensor

data (from e.g., accelerometers) is typically unique to individuals, as well as rich enough to allow for relatively straightforward re-identification [7].

In an ongoing project, we have recently concluded a study with 81 users of a canine activity tracker (FitBark), eliciting any concerns on the use of the device participants may have had, as well as what aspects of these devices were important to them. Amongst others, we asked users how important they found the device's accuracy, consistency, usability, maintainability, scalability, its look and feel, and its security (explained as its ability to preventing information leakage about your dog or you). Security came just-before-last, with only 53% of users finding it important to some extent, 26% being neutral and 21% finding it not important. In contrast, most other aspects were considered important by over 75% of the participants. More telling were the results of open questions asking participants to detail any concerns they have had in their use of the device. A myriad of concerns were elicited – from the ergonomics of the device, to its accuracy, to its poor waterproofing. Yet, not a single participant expressed any concerns about their privacy. This may very well indicate that users are not aware of the potential threats to their privacy – in line with what we focus on in this paper, namely how these devices are marketed as measuring 'only' a pet, not their owner.

What we *did* come across in this study were examples of pet owners using these devices to derive real-world information of third parties from the pet wearable's data. Some of these examples are rather innocuous, such as a person who used the activity patterns of their dog to show it was sleeping during the times that a neighbor mistakenly (or maliciously) issued noise complaints claiming the dog was barking incessantly. In this case data is simply used to (in)validate claims about the actual subject of the measurements: the dog.

However, in other cases users noted interpreting these patterns to infer information about third parties. For example, a different participant described going on business trips regularly and leaving their dog with a dedicated dog sitter, with whom they had an agreement for the exercise goals their dog should achieve while with them. Noting the dog's restlessness on their return, they looked at the recorded activity patterns and saw that the exercise was not met, and on further analysis inferred that the dog moved so little, and so different from its regular patterns, that they had likely been confined to a cage by the dog sitter. This poses a rather unexpected turn: instead of malicious users compromising the users' privacy via attacks, the users themselves potentially compromise the privacy of third parties by interpreting changes in patterns of the wearable's data and associating them with hypothesized actions by that third party. Such indirect observation challenges a key requirement for privacy, namely that people should maintain overall control of their data and its release [8], as well as having to explicitly agree to being tracked. Given these scenarios where pet owners have used a wearable's data to actively infer information about a third party, it is all the more striking they do not seem concerned with similar privacy threats targeted towards them

The key privacy threats discussed above are summarized in Fig. 2, mapped onto the context of pet wearables as shown in Fig. 1. To understand to what extent consumers are exposed to these and potential other threats, we first need to understand what devices are currently on the market, and most importantly, *what* (extent of) data they can be said to

capture. It seems prudent, thus, to investigate *what data pet wearables are known to capture*, and to reflect on the more pressing question: *what privacy implications does this hold?*

3 Market reality: what data do pet wearables capture?

3.1 Wearables on the market

There are many pet wearables available, from official and reseller channels, to seemingly deserted crowdfunder pages. Because no systematic survey or listing of pet wearables is currently available, for purposes of this work we made a (non-exhaustive) selection of products by searching for website and blog posts discussing popular pet wearable products. We included pet wearables if their website had a product available for purchase or pre-order, and offered at least a basic description of functionality, technology, and privacy policy. Table 1 presents an overview of the selected products and their core functionality.

Table 1. Overview of selected pet wearables products, noting (known) data capturing sensors and connectivity.

Device	*Origin*	*Made for*	*Type*	*Interface*	*Sensor(s)*	*Connectivity*
FitBark	US	Dogs	Activity and sleep tracker	App, Web	3-axis accelerometer	Bluetooth
Garmin DeltaSmart	US	Dogs	Obedience trainer, activity tracker	App	*not stated*	Bluetooth
Jagger & Lewis	France	Dogs	Health tracker	App	9-axis accelerometer, microphone	Bluetooth, Wifi
Kippy	Italy	Dogs	Activity and location tracker	App, Web	GPS/LBS	Machine to machine (M2m), network cells
Kyon	Cyprus	Dogs	Location tracker	App	9-axis accelerometer, gyroscope, magnetometer, temperature sensor, altimeter, GPS	Bluetooth, GPRS/3G
Link AKC	US	Dogs	Activity and location tracker	App	3-axis accelerometer, GPS	Bluetooth, Wifi, cellular data (AT&T)
Nuzzle	US	Dogs, Cats	Activity and location tracker	App	GPS	Bluetooth, GPRS/3G
Paby	US	Dogs, Cats	Activity and location tracker	App	GPS/LBS	Wifi, 3G-WCDMA
PawTrack	UK	Cats	Location tracker	App, Web	GPS, GLONASS, Galileo, Beacon tracking	Wifi, GPRS
PetPace	US	Dogs, Cats	Health tracker	App	*"non-invasive sensors"*	*"low power, long range communication"*
PitPat	UK	Dogs	Activity tracker	App	3-axis accelerometer	Bluetooth
Poof (bean/pea)	US	Dogs, Cats	Activity, sleep, and location tracker	App	3-axis accelerometer	Bluetooth
Scollar	US	Dogs, Cats	Activity and location tracker	App	microphone (Scollar trek), GPS	Bluetooth, Wifi, RF
TabCat	UK	Cats	Location tracker	Hardware	-	RF-based
TractiveGPS	Austria	Dogs	Location tracker	App	GPS, GSM	Bluetooth
TractiveMOTION	Austria	Dogs	Location tracker	App	accelerometer, motion detection sensor, temperature sensor, brightness sensor	Bluetooth
Whistle	US	Dogs	Activity tracker	App	3-axis accelerometer, GPS, GLONASS	Bluetooth, Wifi, GPRS/3G
WonderWoof	US	Dogs	Activity tracker	App	3-axis accelerometer	Bluetooth
WÜF	US	Dogs	Activity and location tracker	App	accelerometer, GPS, microphone (conflicting mentions)	Bluetooth, GPRS/3G

Most pet wearables are described as activity and/or location trackers, and with the sole exception of TabCat, all devices typically require the owner to install companion mobile apps

in order to fully use the device. The technology used to subsequently exchange data from the wearable device to the owner's mobile phone is of additional interest, as there is widespread use of Bluetooth, which is still open to multiple attack vectors for data interception [9]. Bluetooth traffic analysis of common fitness trackers has been shown to allow for observation of current activity, and more critically, a user's gait (i.e., their manner of moving), thereby allowing for identification of the observed user [10]. Pet wearables are similarly vulnerable to such analysis, in particular gait analysis, due to the wider breed diversity of dogs making it more straightforward to correlate different gaits with smaller samples of potential dogs. This is a concrete example of the re-identification challenge of sensor data as mentioned earlier, making it feasible to identify pets (and their owners) even in aggregate data sets. Depending on the extent of additional data linked to pets, this may hold significant privacy implications.

3.2 Privacy policy analysis of data captured by pet wearables

For each device, we systematically determined what data they capture of the pet and its owner, detailed in Tables 2 and 3. We first captured a snapshot of each device's publicly available privacy policy. The analysis was performed by two of the authors, who manually extracted the data mentioned in each policy's section on data collection, resulting in a list of terms. This was then iterated over in order to reduce trivial synonyms (e.g., "log in" and "login" being the same). Any terms where it was ambiguous as to what exactly was captured, and whether different terms would relate to the same data (e.g., "activity data" and "exercise data") were left separate. We only considered data collected by the service/devices themselves, not any data collected by third parties such as e.g., Poof's ability to link the wearable to a Facebook account, which would result in an increased scope of data collection. The final set of terms describing captured data was then verified against each privacy policy, noting whether the policy explicitly mentioned capturing such data. Inter-rater reliability was established via Cohen's kappa, with rating for classification of human data $\kappa = 0.93$ and classification of animal data $\kappa = 0.95$, both indicating 'very good' strength of agreement.

This process was first performed in December 2017 and repeated in June 2018 to assess whether the coming into force of the General Data Protection Regulation (GDPR) prompted any policy updates, and, potentially, additional clarification on captured data. Only six devices seem to have had their privacy policy updated since, or close before the GDPR came into force. Those with no updated policies typically have a last modified date (if available) between 2015 and 2017. Several policies lacking a last modified date are out of date regardless, stating compliance with now superseded legislation such as the Data Protection Act 1998, the precursor to the UK's GDPR implementation.

Even though pets are ostensibly the intended users of these wearables, Table 2 shows there is little explicit information on what (if any) data the products capture. Most pet wearables leave things implicit, or use aggregate concepts such as 'activity data,' rather than specifying exactly what is captured. For example, while it would be obvious to most that a wearable stores a pet's name, only three explicitly denote so. We emphasized the mismatch between wearables claiming to track activity, but not explicating what kind of activity data

Table 2. Pet data (not) known to be captured by each wearable. A ✓or † indicates the policy explicitly mentions capturing this data, noted in the first and second analysis, respectively. Empty cells indicate the policy does not explicitly mention capturing this data. A ? indicates an important mismatch, lacking detail on activity or location data in devices with such functionality. Devices highlighted in yellow are not covered by a post-GDPR privacy policy.

device	# of known data captured	name	dob	sex	weight	breed	health	behavior	relationships	photographs	pet profile	activity data	activity goals	biometrics/vitals	exercise data	feeding	location	device sound	adventures	veterinary records	environmental data
FitBark	3										√	√		†							
Garmin DeltaSmart	0											?									
Jagger & Lewis	2										√	√									
Kippy	0																				
Kyon	2										√						√				
Link AKC	5											√	√				?		√	√	√
Nuzzle	0											?					?				
Paby	4	√										√	√				√				
PawTrack	0																?				
PetPace	4										√	√		√	√						
PitPat	14	√	√	√	√	√	√	√	√	√		√		√	√	√	√				
Poof (bean/pea)	0											?					?				
Scollar	0											?					?				
TabCat	0																?				
TractiveGPS	1										†						?				
TractiveMOTION	1										†	?									
Whistle	4	√										√	√				√				
WonderWoof	1	√										?									
WÜF	3											√					√	√			

Note that cells remaining empty or ? are informational – while data is not known to be captured, in many cases it likely is, such as a pet's name, breed, weight, all of which may constitute (sets of) personally identifying information. Their lack of explicit mention in policies thus becomes important to note, as such data is likely not addressed under requirements for personal data processing (e.g., encrypted storage, limitation of transfer).

they capture (shown as empty orange cells), and wearables claiming to track location of pets, but not explicating what kind of location data they capture (shown as empty red cells).

When we switch our attention to what data is captured of owners, more (and certainly more diverse) data is captured. Table 3 shows the extent of owner's (personal) data captured. Here, as well, we marked wearables claiming to track pet location – and thus likely owner location by proxy, but not explicating what kind of location data they capture (shown as empty red cells).

Two points require further analysis. First and foremost, what implications the capturing of particular data by each wearable has. To what extent (and perhaps, why) do some pet wearables capture personal data of the owner such as their gender, location, or hobbies and interests? Second, and perhaps more urgent, what implications does the lack of explicit

Table 3. Owner data additionally known to be captured by the use of each wearable. Markings and colors have the same semantics as in Table 2.

		You																	*Device*			*Content*				*Use of the service*								
device	# of owner data known to be captured	name	gender	age	date of birth	location	address	time-zone	email address	telephone number	social media identifier(s)	relationship to other people	creditcard details	interests	hobbies	pet-related preferences	company name	device identifiers	device configurations	names/version/package IDs of software installed on device	preferences/opinions/(dis)likes	photographs provided to the service	text data provided to the service (reviews, comments, quiz responses)	correspondence with the service	aggregate user data	login information	plan/service status	IP address	cookies	logs	pages viewed	time and usage habits	any other information necessary
FitBark	7	√			†		√		√	†												†					†						
Garmin DeltaSmart	4	√					√			√																							
Jagger & Lewis	3	√					√		√																								
Kippy	0					?																											
Kyon	8	√		√		√	√		√			√							√	√													
Link AKC	17	√				?	√		√	√							√	√	√	√		√	√	√	√		√	√	√	√	√	√	
Nuzzle	4					√	√																					√			√		
Paby	10	√			√	√			√								√	√			√	√			√		√						
PawTrack	5	√				?	√		√	√			√																				
PetPace	1																									√							
PitPat	15	√	√		√	√	√		√	√	√							√		√	√	√			√				√	√		
Poof (bean/pea)	3					√			√																						√		
Scollar	20	√	√	√		?	√	√	√		√			√	√	√		√	√	√			√		√		√	√	√	√	√		
TabCat	0					?																											
TractiveGPS	9	†			†	†	†		†	†													†					†	√				
TractiveMOTION	9	†			†	†	†		†	†													†					†	√				
Whistle	14	√				√		√	√									√	√				√			√		√	√	√	√	√	√
WonderWoof	12	√				√	√		√	√			√						√							√		√	√		√	√	
WÜF	10	√			√		√		√	√								√	√									√			√	√	

mention in privacy policies whether data is captured have? The sheer number of empty cells in both Tables 2 and 3 indicate that consumers will be at a loss for reasonably inferring to what extent their privacy may be at stake.

4 Discussion: concerns for the use of pet wearables

In this section we discuss several concerns specific to pet wearables that arise from the above findings. This does not imply these are the only (privacy related) concerns, as well known general issues are equally as problematic here, and may in fact exacerbate them – such as data access, (e.g., WÜF's privacy policy noting that "[collected data] is generally not available to customers for their own, direct access."), and data removal (e.g., PawTrack's inserting of a conditional "where appropriate" clause to any personal data modification requests).

Mismatch between how products are marketed and what data they track. There is a mismatch between product marketing and their data collection in two ways: on the one

hand they capture more than one would expect, and on the other hand they do not detail capturing key data one would expect being captured, such as location by a location tracker device.

To describe the first kind of mismatch, we direct attention to those devices which are explicitly marketed as being activity or fitness trackers with no location tracking capabilities, but, through the use of its necessary related app, end up tracking their owners' location regardless. For example, *WonderWoof* is marketed to consumers stating, among others, "the WonderWoof BowTie does not have GPS and does not track your dog's location in real time." However, the location of the human user is tracked, as can be seen in Table 3. As argued before, due to the close relationship between humans and their pets, specifically dogs, this practically means that the location of a dog wearing this device *is* tracked during a big part of the day.

This is not the only device to do so. PitPat, for example, similarly answers a frequently asked question whether the device tracks dogs' location by "No, PitPat is an activity monitor (walking, running, sleeping, playing etc) and does not have GPS." Yet, similarly, the accompanying software does track the location of the human user. Knowing that PitPat explicitly claims to have business partners in areas such as "pet insurance; pet food/ supplements/pharmaceuticals; veterinary care; retail; academic and other research," the location of dogs and their owners may indeed be valuable data that owners are not aware of being used in such a way.

Post-GDPR the capture of location data remains one of the better examples of ambiguity as to whose data is captured. Tractive's privacy policy details that they do, indeed, capture location. However, it states only: "GPS position of the user's mobile device (for showing the user position on the map)" But what of the GPS of the pet wearable itself? Surely this is to be shown on a map as well, for example to find a lost pet. No such mention is made, even though a dog will typically be in close proximity to its owner, making tracking the dog's location equally as privacy sensitive as tracking a mobile phone. To further confuse matters, the policy does note that the purpose of its data processing includes "track[ing] your pet's location" – without detailing that they actually capture the data to do so.

A rare positive example can be found in Kyon's policy, which seems to understand and warn users of the potentially sensitive nature of pet location data: "the location of your KYON tracking collar and base station, geo-fence information which may disclose the location of your residence or other locations personal to you".

The second kind of mismatch is a lack of clarity as to whether expected data is captured or not. Tables 2 and 3 show those devices marketed as activity and/or location trackers which do not explicate what, or the extent of, such data is captured. This makes it difficult to verify the extent of data collected, and what information may be deduced from it. For example, PawTrack is marketed as "the world's most advanced cat tracking system," boasting incorporating Gallileo, Glonass and GPS, making it possible to track a cat where ever they are. Yet, regardless of all the sensors the device contains and the potential data collection it performs there is not a single mention of location in its privacy policy. As a result, it is not possible to establish whether location data is captured constantly, intermittently, and so on.

The TractiveGPS pet tracker similarly markets itself as a GPS tracker enabling tracking the exact location of a pet, and uses boasts "LIVE tracking," but, again, does not elaborate in its privacy policy on the extent of location data captured.

> **Key finding:** looking at a pet wearable's functionality is not enough for a user to feasibly assess the kinds and extent of data it captures.

Differences in whether pet data is classified as personal data. Some devices implicitly acknowledge the sensitive nature of data collected from pets by mentioning it as personal data collected. For example, FitBark notes that personal information includes "your dog's profile and activity information." Some devices remain vague on the matter, especially when they do not list any data captured, as will be discussed below. However, one wearable stands out from its contrasting position. The privacy policy of PetPace explicitly states:

> "Pets' Data is non-identifiable nor shall be considered as personal information."

As argued before, because in the use of pet wearables the collection of human data and animal data are integrated and processed by a single device, there is very little reason to assume the animal data does not have a relation to an identifiable natural person.

> **Key finding:** some pet wearables do not consider the sensitive nature of pet data captured via pet wearables.

Unclear extent of what animal data is stored (and inferred) In line with findings that privacy policies are rife with vague and unclear language [11], we encountered two types of concerns where consumers cannot be sure of the extent of data collected by the wearable.

First, several devices do not state at all what (personal) data is collected, such as the Garmin DeltaSmart, Kippy, Nuzzle, PawTrack, Poof, Scollar, and TabCat. This is a concern because we cannot infer whether animal data that is collected by the device is considered as personal data or not. For example, the Garmin privacy policy states that personal information is "information that, either alone or in combination with other information collected, identifies an individual." This would reasonably include most, if not all, animal data. Yet, as also shown above, not all device manufacturers would agree with this interpretation, making it impossible to determine to what extent animal data is suitably protected.

Second, several devices describe what data is collected in terms of combined or aggregate concepts. For example, FitBark, Jagger & Lewis, Kyon, Paby, PetPace, WÜF all use concepts such as 'pet profile' or 'activity data' to describe what animal data is gathered, rather than detailing this to exact data. This is of concern because one cannot infer how critical the animal data collected is. Nonetheless, several of such devices do note the sensitive nature of animal data, such as Paby, which notes that personal information processed by the device includes the pet's 'activity data' and its 'activity goals'.

This has not abated in the policies updated since the advent of the GDPR, from FitBark adding that they capture "your dog's health and behavioral information," without detailing

what that information is, or the updated policy for TractiveGPS and TractiveMOTION referring to the notion of "pet related data," which is only defined as: "... allows to draw conclusions about the pet owner (e.g. pet chip id)." This lack of transparency gives little information as to exactly what pet information is captured, and to what extent it may identify the pet's owner. This makes it difficult for owners to assess whether they are comfortable with the wearable's data capture, let alone understand how much their privacy is potentially at risk.

Key finding: consumers cannot be sure of the exact data that is collected and stored by their pet wearable.

5 Implications: what are the key privacy threats that need to be dealt with?

5.1 The extent of personal data captured by pet wearables is seemingly misrepresented

When a device is marketed as solely an activity tracker, and makes several mentions (in e.g., product descriptions, and official FAQs) that they do not include GPS, and do not track the pet's location, it is absolutely reasonable for a consumer not actually wearing the device to infer that normal use of the wearable would not track their, or their pet's location. However, as shown in Table 3 this is not always the case. This holds not only for location, but also other sensitive personal data, where it is not reasonable for the consumer to assume such information would be tracked and stored.

Compare this to the scenario, discussed above, of unintentional data leakage via FitBit and Strava. In that case, military personnel tracked their exercise routes and data, and knowingly uploaded it to a third party service which specifically mentioned using any such data. In such cases it can be argued that users could *reasonably* have understood the privacy risk, given the known sensitivity of the data. However, what of such scenarios when one is not aware of the extent of personal data gathered by the devices which does not seem reasonable? Why would someone expect their location to be also tracked if uploading e.g., animal data of a device noted not to have GPS, nor track the animal's location? Moreover, one cannot feasibly infer whether data is sensitive if aggregates such as "activity data" or "pet profile" are used – all of which may, for example, include (indirect) location estimates.

Better protection of consumers is needed by ensuring that devices whose key data capturing subject is a person, do not market themselves as targeting an entirely different entity, the pet.

5.2 Consumers and third parties are potentially at risk due to the lack of classification of animal data's status as personal data

If companies explicitly classify collected animal data as not personally identifiable, and therefore not protected under relevant data protection clauses, such data is at risk. Several devices

avoid mentioning animal data as personal data, or use aggregate concepts that make it difficult to assess exactly what data is protected. This poses a risk towards users of pet wearables due to the potential of inferring sensitive data of the human from the pet's data.

Such risks are known and well studied, such as the tracking of mobile phones now being equated with tracking their owner. Research has shown other contexts in which personal data could be inferred from seemingly non-personal data, such as deriving the specific train route someone travels by from patterns in their phone's vibration energy harvesting system [12]. Because the human-animal companionship between owners and their pets is well known, any animal data should be carefully assessed for its potential to indirectly reveal identity or other information about the related human.

The examples given in Section 2 make it clear that even if there are no well-known cases of owner's privacy being violated by pet data, they themselves already use this data to infer information about third parties from the data captured of their pets. This raises further discussions on how to interpret such data (and how to agree on such interpretations), as in the absence of certification schemes for accuracy of wearables, inaccurate data may lead one to misjudge a third party's behavior. In the earlier dog sitter scenario, what would happen if the wearable's classification algorithms were not optimal and misclassified the dog's behavior – leading the owner to accuse a third party of malicious behavior, with false, but hard to repudiate proof?

Moreover, an increasing number of pet wearable manufacturers are entering into collaborations with larger corporations. For example, Whistle was recently incorporated into the Mars Petcare veterinary health group which includes a significant number of third parties in pet nutrition, healthcare, and insurance.Vodafone recently incorporated Kippy into the V by Vodafone range of services which tracks consumers' pets, children, cars, and other possessions.While such integration is ostensibly for direct consumer functionality and wider social benefit (e.g., improving pet healthcare), as a result large datasets incorporating data of pet wearables may become available to a wide range of third parties.

This shows the need to explicitly protect animal data as personal data, both to protect people from having their personal data compromised by malicious attackers, as well as those same people unintentionally opening themselves up to liability by unknowingly compromising the privacy of others by deriving personal data on them through their pet's data.

6 Conclusion

This article has shown that pet wearables on the market engage in extensive data collection of their human owners typically capturing far more data of the owner via the accompanying software than of the pet itself and tend to be vague on the extent of pet data collected all of which may be sensitive and lead to the identification of people the pet has interacted with. We argue that consumers are led into underestimating the extent of personal data collected, and that they may be at risk due to the denial of pet data's status as personal data.

With the increase of strict data privacy laws being passed around the world, and the now active enforcement of the GDPR – applicable to any company processing data of EU citizens, it seems particularly timely to stimulate a discussion on what extent of pet wearable

data is personal data, and how it should be suitably protected. Comparing our findings with the GDPR's key principles for personal data processing:

Mismatch between how products are marketed and what data they track: capturing more data than expected violates the principle of data minimization which requires the capture of personal data to be not only adequate and relevant, but also limited to what is necessary.

Differences in whether pet data is classified as personal data: actively denying pet data being personal data or doing so implicitly by not detailing any captured pet data in privacy policies violates the key definition of personal data: any information *relating* to an identified or identifiable natural person, especially because these devices typically capture direct personal identifiers (i.e., the owner's details).

Unclear extent of what data is stored (and inferred): the lack of detail on what data is captured, or the use of ambiguous aggregate concepts violates the principle of transparency which requires clear and plain language regarding what data is captured, and what the consequences of processing that data will be.

Implementing privacy controls could mitigate some of these concerns, by giving consumers clearer insight into what data is captured and allowing them to opt-out of non-vital data capture (i.e., much of the data in Table 3). More complicated, however, is the matter of stored pet data reflecting personal data not only of its owner, but of other people with whom the pet interacts. Privacy controls, through nudging [13], could be a solution for third parties knowingly interacting with the pet, such as a family member while pet-sitting. They could install the wearable's app and be given temporary access to privacy controls by the pet owner while in the vicinity of the pet, so that while pet-sitting they would maintain control over the extent of data captured.

However, third parties that do not knowingly interact with the pet could not feasibly do so. To protect their right to privacy, a combination of policy and responsible use, informing the owner via nudges seems a more viable solution. For example, nudges could describe the potential consequences that processing of this data may have – "you're in public now: your dog's activity data may disclose information on others it interacts with!" Rather than relegate such warnings to privacy policies that go unread by most consumers, using nudges when using relevant functionality would go a long way in ensuring consumers realize the potential impact of using these wearables.

As manufacturers of pet wearables on the market differ in their views towards pet data, from acknowledging its sensitive nature and ability to identify people to outright denying it (with most manufacturers seemingly avoiding an explicit stance on the debate), we call for explicit discussion and policy towards the secure treatment of pet data. We need more insights to understand what pet data (or combinations thereof) can be considered personal data, when and how it can be shared or transferred to new or other owners, and how we can protect the impact such data has on both pet owners and third parties whose behavior and actions may be indirectly reflected in such data.

References

1. Vivian Genaro Motti and Kelly Caine. Users privacy concerns about wearables. In *International Conference on Financial Cryptography and Data Security*, pages 231–244. Springer, 2015.
2. The Guardian: Fitness tracking app Strava gives away location of secret US army bases. `https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases`. Online; Accessed: 09 May 2018.
3. Florian Rheingans, Burhan Cikit, and Claus-Peter H Ernst. The potential influence of privacy risk on activity tracker usage: A study. In *The drivers of wearable device usage*, pages 25–35. Springer, 2016.
4. Nanna Gorm and Irina Shklovski. Sharing steps in the workplace: Changing privacy concerns over time. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 4315–4319, New York, NY, USA, 2016. ACM.
5. Malte Spitz. Your phone company is watching you. `https://www.ted.com/talks/malte_spitz_your_phone_company_is_watching`, 2012. Online; accessed 12 January 2018.
6. Cassim Ladha, Nils Hammerla, Emma Hughes, Patrick Olivier, and Thomas Ploetz. Dog's life: wearable activity recognition for dogs. In *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*, pages 415–418. ACM, 2013.
7. Scott R Peppet. Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent. *Tex. L. Rev.*, 93:85, 2014.
8. Nigel Davies, Nina Taft, Mahadev Satyanarayanan, Sarah Clinch, and Brandon Amos. Privacy mediators: Helping iot cross the chasm. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*, HotMobile '16, pages 39–44, New York, NY, USA, 2016. ACM.
9. Wahhab Albazrqaoe, Jun Huang, and Guoliang Xing. Practical bluetooth traffic sniffing: Systems and privacy implications. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '16, pages 333–345, New York, NY, USA, 2016. ACM.
10. Aveek K. Das, Parth H. Pathak, Chen-Nee Chuah, and Prasant Mohapatra. Uncovering privacy leakage in ble network traffic of wearable fitness trackers. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*, HotMobile '16, pages 99–104, New York, NY, USA, 2016. ACM.
11. Pauline Anthonysamy, Phil Greenwood, and Awais Rashid. Social networking privacy: Understanding the disconnect from policy to controls. *Computer*, 46(6):60–67, 2013.
12. Marzieh Jalal Abadi, Sara Khalifa, Salil S Kanhere, and Mahbub Hassan. Energy harvesting wearables can tell which train route you have taken. In *Local Computer Networks Workshops (LCN Workshops), 2016 IEEE 41st Conference on*, pages 199–204. IEEE, 2016.
13. Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 787–796. ACM, 2015.