“Some might freak out” – What if your dog’s activity tracker were to have a data breach?

Dirk van der Linden, Emma Williams
University of Bristol
{dirk.vanderlinden,emma.williams}@bristol.ac.uk

Irit Hadar, Anna Zamansky
University of Haifa
{hadari,annazam} @is.haifa.ac.il

ABSTRACT

Activity trackers for dogs are increasingly popular, having the potential to improve pets’ welfare and providing a ‘digital voice’ for expressing their needs. ACI research has so far mainly focused on their impact on the pet-human bond. However, also privacy considerations play an important role as they may pose significant barriers towards their wider adoption. We report on a mixed-method study (N=61) investigating what, if any, privacy concerns dog owners hold towards the data captured by their dog’s device.

We elicited detailed reflections by participants towards the consequences for themselves and others of a hypothetical data breach leaking their dog’s data. In addition, we captured several potential indicators for the perception of consequences: trust, perceived transparency, risk, benefit, and self-assessed knowledge of dog behavior (and thus its data). Statistical analysis of the findings indicated that perceived consequences were moderately correlated with trust and perceived benefit of use for society as a whole. A thematic analysis revealed that participants either did not see any consequences, saw consequences only when reasoning about others, or saw consequences to their own or dog’s safety, rather than their privacy.

We discuss why these findings are worrying in light of the information asymmetry between consumer and service provider, setting out an argument why dog owners should care more about dog activity data and its privacy implications due to the data’s ability to reveal potentially sensitive data about themselves as well as their caregiving.

ACM Classification Keywords

Security and privacy: Social aspects of security and privacy

Author Keywords

wearables; ACI; pet; dog, privacy

INTRODUCTION

Pet wearables are increasingly prevalent. One of the most popular types of device on the market are activity trackers for dogs [10]. Many of these devices are marketed explicitly as tools that aid in both dog and human health, providing information to guide users towards healthy levels of exercise, diet, and sleep, as well as catch early signs of discomfort or disease and monitor rehabilitation. These devices are gaining increasing attention of the ACI community due to their potential of strengthening the pet-human bond (cf. [40, 44]). However, it is also important to investigate factors that may pose barriers to their wider adoption.

One such factor are privacy implications of these devices which have received some initial attention [41]. However, users’ concerns about privacy, and in particular, data captured by these devices, have not been addressed in detail.

Given the focus of dog activity trackers on dog health data, the close connection between dog and owner, and the potential for dog activity data to (indirectly) reflect the owner’s, or even bystander’s, routines [41, 45, 44], it is important to understand to what extent consumers are aware of the potential privacy implications, and whether they take adequate measures to use these devices in a privacy-preserving way.

To address this, we conducted a mixed-method study with users of a popular dog activity tracker. We investigate consequences seen by dog owners should their dog’s activity data leak, and how this relates to several validated indicators, including perceived trustworthiness, transparency of data policy, and perceived risk/benefit of using the device. Through complementary quantitative and qualitative analysis of the elicited data we explore the following research questions:

RQ1. What privacy concerns do dog owners perceive for pet activity data?

RQ2. Are there any predictive indicators for the appearance of such privacy concerns?

RQ3. What explanations underlie the extent and type of privacy concerns expressed about pet activity data?

The contribution of our work includes:

A quantitative and qualitative analysis of factors related to perceived consequences of dog activity data breaches. Participants perceive a range of potential consequences, including significant safety threats as pet theft and burglary, while seeming to see them as consequences that other people will suffer from. Potential consequences are correlated with the perceived benefit of use of a dog activity tracker, as well as the extent to which the device’s manufacturer is considered trustworthy.

A discussion of factors that dissuade consumers from reasoning about impact on their own privacy. We found many

ACI’19, November 12–14, 2019, Haifa, Israel

ISBN 978-1-4503-7693-8/19/11. . . $15.00
DOI: http://dx.doi.org/10.1145/3371049.3371057

participants showed a mental focus on safety rather than privacy, to the extent that 'safety alone' would be a better characterization than 'safety first'. Moreover, many participants likely overestimate their level of knowledge relevant for understanding dog activity data, which in turn is likely to negatively affect their ability to perceive potential threats.

A discussion of the apparent disconnect between consumers and service providers in realizing the value of dog activity data. Participants noted seeing little value of dog activity data, and holding little concern towards its leaking or use by others. Yet, device manufacturers and service providers *do* seem to see value in this data, as evidenced by a growing number of data ecosystems in which such valuable data is shared with third parties such as veterinarians, insurance companies, pet food producers, and other pet service providers.

RELATED WORK

People and their dogs

The bond between human and animal has been well established in research. Contact with animals has been shown to have a significant positive effect on psychological and physiological human health [6]. Pet ownership has been shown to contribute to health and perceived happiness [42], in no small way by encouraging joint physical activity [11, 9]. The increasing popularity of activity trackers for companion animals (cf. [10]) should thus come as no surprise.

As close as pets and their owners may be, there is a significant cross-species language barrier. Research has shown that dog owners overestimate their understanding of dogs' emotional state and behavior, failing to accurately interpret the behavioral signals sent by dogs [23]. Similarly, research has shown that dog owners were not likely to identify early signs of problematic behavior, challenging the idea that mere exposure to dogs without any theoretical knowledge of behavior is sufficient for adequate behavioral understanding [38]. Another study found that, when shown a video of dogs interacting with a tablet-based video game, dog owners with no expertise in dog behavior were more prone to generalization, and less effective at understanding the dog's behavior [46]. These activity trackers may thus additionally serve a role of strengthening the human-animal bond by informing owners better of their dogs' physiological state.

The activity data these devices generate with simple accelerometers alone – let alone when equipped with additional sensors – has been shown to allow for detailed classification of complex dog behavior and geo-spatial positioning [25]. This allows for the deduction of more complex cognitive and emotional states of a dog as well, for example deducing with a certain degree of certainty whether the dog was in a position where they physically expressed fear. Given additional information of the people in the vicinity of a dog, such data could have clear implications. However, there remain numerous privacy and security considerations in regard to the use of these devices. Mozilla's "*privacy not included"[1] project shows several extant Bluetooth Low Energy (BLE) vulnerabilities in pet wearables that allowed for data interception and man-in-the-middle attacks [39].

A review of the privacy policies of several commercially available pet wearables [41] showed that there is a critical mismatch between how these devices they are marketed and their transparency in what data they captured – six devices with activity tracking functionality did not detail any pet activity data in their privacy policies, while seven devices with location tracking functionality did not detail any location data in their privacy policy. Moreover, most devices were shown to capture more owner data than pet data, and remain unclear about what pet activity data is actually stored. A study among people raising candidate blind guide dogs for a guide dog center found they were divided on the question of whether dog activity data from such trackers constitutes personal data [45]. Moreover, a study with 81 dog owners using a popular commercial activity tracker showed that very few, if any dog owners professed any interest in security as a requirement that would influence their decision to purchase and use the device [44].

People and their data

One of the key privacy concerns consumers have, and which continues to increase in significance [5] is how their personal information is stored, accessed, and transferred [14]. At the same time, consumers typically consider privacy and security implications only *after* purchasing wearable technology [15].

To understand how consumers perceive this privacy and security implications, exploring the mental models that characterize stakeholders' privacy and security concerns has been noted as an effective way to understand the privacy needs of users [19]. Many studies have been performed to explore such mental models. Kang et al. [21] showed that technically less experienced people had simpler mental models, and as a result perceived less privacy threats. Yet, there was no direct relationship between technical experience and preventive (privacy preserving) actions taken by users. A study of user privacy concerns in smart homes similarly found gaps in threat models arising from users' limited technical understanding of smart home technology [47]. An investigation of folk theories of sensor data collection showed that perceived visibility of data types is related to how (much) users interact with them [32]. The need for greater transparency on inferences enabled by data aggregation (let alone primary capturing) has been argued to be necessary to empower users in understanding what data may reveal about them [33] – certainly relevant in the context of dog activity trackers given the above discussed richness of even simple accelerometer data.

Privacy expectations and preferences in a general IoT context have been shown to be diverse and context dependent, with most users in particular being more comfortable with sensor-driven data collection in public rather than private settings [27]. At the same time, people have also been found to feel a heightened state of being surveilled by their peers, adopting privacy-preserving workarounds in specific known contexts such as pervasive photography [34]. An exploration of experiences of online privacy-related panic events showed that when users realize that their personal data leaking or being obtained by someone they do not approve of was the second-most reported

[1] See:https://foundation.mozilla.org/en/privacynotincluded/categories/Pets/

panic story, beaten only by account hacking or hijacking [4]. A survey of people's comprehension of data breach risks and their sentiment towards remediation steps found that users readily understand the risks of data breaches [22]. Yet, other research in the context of credit bureaus showed that people's mental models of the domain were incomplete and partially inaccurate [49]. People were not sure if they were affected by data breaches, and very few took protective measures, which was linked to the cost of protective measures, optimism bias ("it won't happen to me"), and a general tendency of delaying action until harm has occurred.

STUDY DESIGN

Materials

The study was designed to elicit quantitative and qualitative data on the variables shown in Fig. 1, to both allow for the qualitative study of what consequences participants perceived with regard to data breaches, and the extent to which hypothesized relationships between variables could be found.

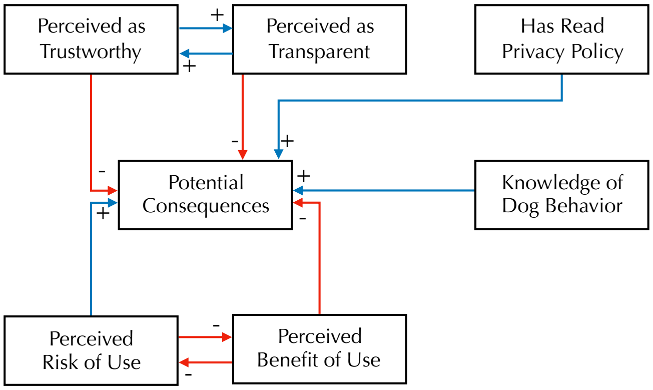


Figure 1. Studied variables and hypotheses.

The study was designed as a questionnaire incorporating both Likert scale and open-ended questions. We iteratively designed the study with a behavioral veterinarian whose patients have used these devices. Feedback indicated the survey completion time was around ten minutes, depending on the level of detail provided to the open questions. The questionnaire elicited the following data:

- What is your dog's:
  - name
  - breed
- *Indicator for Trust* (adapted from [30]):
  On a scale from 1 (strongly disagree) to 5 (strongly agree), how much do you agree with the below statements?
  - [**Device**] is honest in providing accurate information about what data they capture [1–5]
  - For me, getting accurate information about what data [**Device**] captures is [not at all–extremely important]
- *Indicator for Perceived Transparency* (adapted from [30]):
  On a scale from 1 (strongly disagree) to 5 (strongly agree), how much do you agree with the below statements?
  - Getting information about what data [**Device**] captures would be easy [1–5]
  - For me, getting information about what data [**Device**] captures is [not at all–extremely important]
- *Elicitation of potential consequences from data breach*:
  Assume that hackers managed to access [**Device**] servers and published the activity data of a large number of dogs – yours included online, for anyone to browse.
  - In your view, what are the potential consequences of such a leak for you? [max 500 words]
  - In your view, what are the potential consequences of such a leak for others? [max 500 words]

  (both adapted from [49])
- *Perceived Risk and Benefit* (adapted from [1])
  - In general, how risky do you consider [**Device**] to be for: [not at all risky (1)–very risky (5)]
    - Your dog
    - Yourself
    - Your social circle
    - Society as a whole
  - In general, how beneficial do you consider [**Device**] to be for [not at all beneficial (1)–very beneficial (5)]
    - Your dog
    - Yourself
    - Your social circle
    - Society as a whole
- *Demographic questions*:
  - How long have you used [**Device**]? [days/weeks/months/years]
  - Have you read [**Device**]'s privacy policy? [yes/no]
  - How would you rate your knowledge about dog behaviour in general? [1–5]
  - What is your age?
  - What is your gender? [male/female/other]

Participants

We obtained approval from our Institutional Review Board (IRB) before any empirical work began. Sixty-three users were recruited via an invitation to our study posted on an active brand-specific international social media group, where users discuss their experiences and questions regarding the brand's specific device for tracking their dog's activity. No personal details were recorded. All participated voluntarily and received no compensation for their participation.

Analysis

Correlation in the ordinal data was analyzed using estimation of polychloric correlation co-efficient with the *R* 'polycor' package. Binomial tests were used to analyze distribution of responses after reducing valence to categorical data.

Qualitative data elicited in the open questions was assessed by closed coding for targeted purposes (assessing whether consequences indicated an actual privacy concern), and thematic analysis for in-depth exploration of the explanations that underlie the concerns. A codebook was established by two authors following Braun and Clarke's approach to thematic analysis [8] focused on the data related to potential consequences, leading to the codebook depicted in Fig. 5.

Limitations

Internal validity

For the indicators we took care to adapt validated items from other studies, as referenced in the Materials section. This approach cannot be adopted as straightforward for the open questions: here we used two authors independently reading responses to verify whether the answers were in the range of expected outcomes. We found that answers to the second data breach question, what consequences a leak would hold for others, was interpreted differently by all participants (how third parties suffering from a leak would react, rather than how third parties would be impacted by a leak of the participants' dog's data), and adjusted our interpretation of the data accordingly.

External validity

We used purposive sampling to only include users of a specific device, in order to avoid the threat of the sample describing attitudes towards functionally distinct devices, marketed in different ways to their users. Using a purposive sampling approach targeting users of a specific product limits generalizability to some extent, however, the combination of using an international widely frequented social media group, as well as the product being one of the most popular devices available, allowed us to perform exploratory work focusing on the established research questions, rather than attempting to generalize them to universal conclusions.

Ecological validity

We investigated actual users of the device, whereas many existing studies use general population, or even people using similar devices on other species. A concern can be raised over the phrasing of the question, postulating a hypothetical data breach, rather than being able to point users towards a concrete data breach. However, we feel that given the prevalence of well-reported data breaches (no doubt in thanks to the GDPR's mandatory data breach reporting requirements), participants are not asked to make a major conceptual leap in accepting this hypothetical scenario.

FINDINGS

A total of 63 results were elicited. We removed two responses; one due to suspicious data patterns, another due to a participant entering the same answers separately for both their dogs. The final dataset contained *n*=61 responses.

Demographics

As shown in Table 1, participants were predominantly women (89%), median age 35±13 years, with a balanced distribution in how long they have been using the device. This gender imbalance is consistent with reports from the behavioral veterinarian we consulted in terms of what member of the household takes care for the companion animals upon themselves. Participants' dogs were active to varying degrees, most sufficiently for the activity monitoring to realistically capture indirect data of others.

Table 1. Demographic data.

		$(n = 61)$
Gender	Male	10%
	Female	89%
	No answer	1%
Age	18 – 24	7%
	25 – 34	33%
	35 – 45	18%
	45 – 55	20%
	55 – 65	10%
	65+	2%
	no answer	11%
Dog's activity level	0 hrs	3%
	0–1 hrs	25%
	1–2 hrs	55%
	2+ hrs	17%
Used the device for	Days	11%
	Weeks	28%
	Months	33%
	Years	28%
Read privacy policy?	Yes	36%
	No	64%

Quantitative findings

Descriptive statistics

Figure 3 shows to what extent participants perceive the device manufacturer to be trustworthy and transparent in regard to its data capture. Most participants were quite confident in their self-assessment ratings, with perceived trustworthiness (median=4 $\pm$ .5), transparency (median=4 $\pm$ .81), and self-assessed knowledge of dog behavior (median=4 $\pm$ .72) all rated highly. The result data were reduced to categorical polarities to run a binomial test to verify they differed from chance (.5) distributions, which was the case for all variables at $p < .0001$.

Figure 4 shows the distribution of perceived risk and benefits for different parties. The expected inverse relation between perceived risk and benefit holds for risks perceived for the dog as well as self, with low risk (median dog=1 $\pm$ .87; self=2 $\pm$ 1.02) and inversely high benefit (median dog=5 $\pm$ .76; self=5 $\pm$ .77). However, for perceived risk/benefit outside of participants themselves this relationship becomes muddled: risk/benefit for participants' social circle was $1 \pm .76/3 \pm 1.40$ and for society as a whole $2 \pm 0.9/4 \pm 1.19$. Moreover, binomial tests were used to verify these results differed from chance (.5) distribution, which was the case for all variables at $p < 0.001$, *excepting* perceived benefit for society as a whole, which did not differ from chance levels ($p = .152848$). This may indicate a less developed mental model of the risks and benefits for society as a whole.

Additionally noteworthy is the difference between perceived benefit for participants' social circle as opposed to society as a whole: participants are less sure when it comes to benefits for their social circle, while being more sure for society as a whole. This may indicate abstract reasoning in the latter, while they attempt to define concrete benefits for their social circle linked to concrete identifiable persons.

Correlation analysis

Analysis of estimated value of polychloric correlations showed several statistically significant negative correlations between the investigated variables, summarized in Fig. 2.

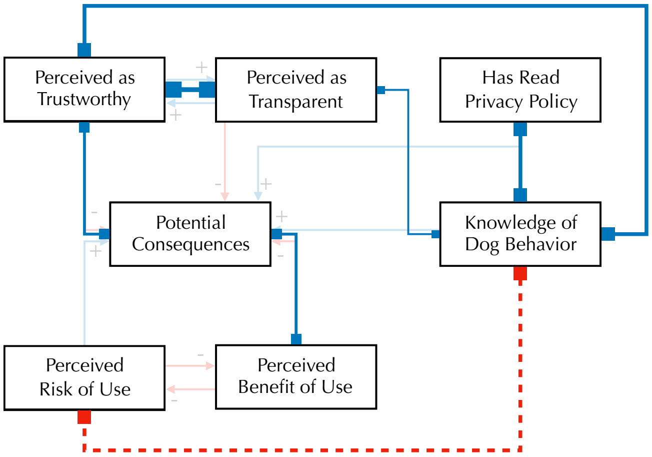


Figure 2. Correlations between variables, positive *r* blue, negative dotted red, line width indicating strength of *r*

The indicators for trust and transparency were both correlated (p<.05) with its additional measurement of the importance of that indicator (r=0.42, 0.49). Moreover, trust was correlated (p<.01) with perceived transparency (r=0.57).

Consequences were moderately correlated (p<.05) with trust (r=0.39), importance of transparency (r=0.39), and perceived benefit to society (r=0.33).

Self-assessed knowledge of dog behavior was correlated (p<.01) with trust (r=0.48), and, correlated (p<.05) with importance of trust (r=0.34), transparency (r=0.29), whether participants read the privacy policy (r=0.43), and negatively correlated (p<.05) with perceived risk to dog (r=−0.42), perceived risk to self (r=-0.38).

Moreover, internally perceived risks and benefit were strongly preserved, with all risks being strongly correlated (p<.01) to other risks (r=0.71 to 0.91). Perceived benefits were somewhat less strongly correlated (p<.01) to other benefits (r=0.39 to 0.74).

Table 2 contrasts the hypothesized and found correlations between perceived consequences and the investigated variables. Our findings indicate the opposite of what we had hypothesized; more consequences are perceived when the device manufacturer is perceived as trustworthy, and when the benefit of use is perceived to be higher. These findings and their implications will be discussed in more detail in Sec. 5.1

Qualitative findings

Independent coding by two authors (Cohen's κ=.824, indicating very good inter-rater reliability) of the elicited consequences showed 37% of the elicited responses contained actual consequences, with the remaining 63% of rejecting consequences arising from a data breach. Fig. 5 shows the codebook and themes found in the thematic analysis.

Table 2. Hypothesized vs. found relations.

Consequences and . . .	Hyp	Real
. . . Perceived as Trustworthy	−	+
. . . Perceived as Transparent	+	∅
. . . Has Read Privacy Policy	+	∅
. . . Knowledge of Dog Behavior	+	∅
. . . Perceived Risk of Use	+	∅
. . . Perceived Benefit of Use	−	+

The quantitative analysis revealed only three moderate correlations to whether any privacy consequences would be perceived: the perceived trustworthiness of the manufacturer, the importance of perceived transparency of the manufacturer's data policy, and, less obviously, the perceived benefit of the device's use to society as a whole. The lack of further correlations that could explain whether participants would perceive any privacy consequences may be due to the significant skewing of most results towards strongly positive or negative values (most participants deeming the company trustworthy and transparent, highly self-assessing their knowledge of dog behavior, not having read the privacy policy).

The qualitative analysis of the participants led to a more nuanced view of their mental models, indicating that there is at first a split as to whether consequences are perceived at all, for differing reasons, followed by increasingly granular consequences, often seen as more likely to happen to others rather than themselves. On a high level, we divided these into themes characterized by one of the following:

1. **No consequences**: nothing bad happening;
2. **Consequences for others**: bad things happen to others;
3. **Consequences for me**: bad could things happen to me.

The below sections will explore in more detail the individual themes that arose in these three interpretations, and how they may explain the type and extent of privacy concerns that participants expressed.

No consequences

. . . and I don't need to rationalize that.

Almost a third of participants (29%) confidently claimed there would be no consequences from such a data breach, without offering any rationale towards it.

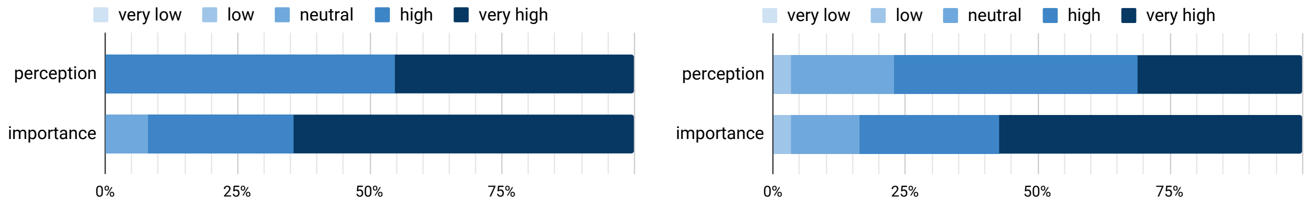
> "None. I had assumed it was all publicly available already." (P44)
> "Not a big deal." (P4)

Some were even quite confident that instead of anything bad happening, the consequences would only be positive, albeit for the device manufacturer:

> "Nothing, it would probably help sell [device brand]! Exposure" (P31)

. . . because my dog's activity isn't sensitive, right?

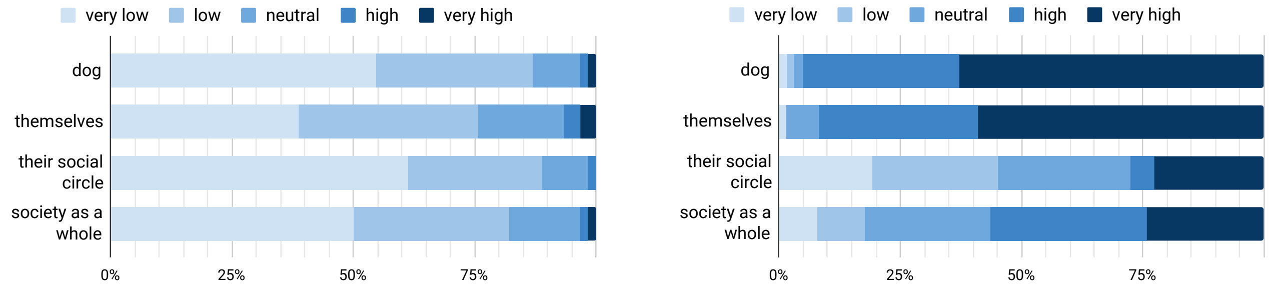
Many participants also reasoned that there would be no consequences if, or because they do not perceive the leaked data as personal data.



(a) Trust

(b) Transparency

Figure 3. Distribution of perceived trust and transparency of device manufacturer.



(a) Risk

(b) Benefit

Figure 4. Distribution of perceived risk and benefit of device use.

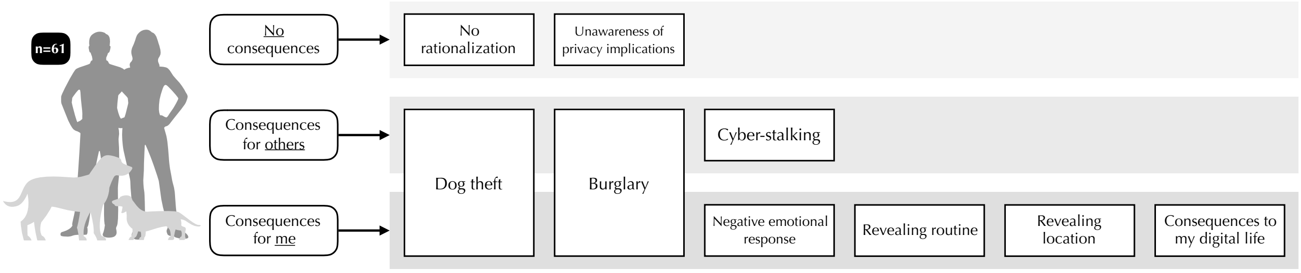


Figure 5. Schematic depiction of the codebook arising out of the thematic analysis.

For example, P1 contrasted the leaked dog activity data with more important data, noting that such a leak would be "not too important, unless my personal information was found."

Dog's activity data was indeed explicitly phrased as not sensitive data, for example:

> "If only activity data was accessed basically none but if account info was then serious." (P28)
> "nothing for my pup's activities, if they want to know, go for it :D" (P29)

Some participants characterized in more detail what data types they would only be concerned about leaking, typically raising the issue of location data, such as P33 noting that unless the leak covers "[...] tracking location, which I don't believe it does, then I don't feel it would have much consequence."

Consequences for others

Strikingly, several participants did not verbalize any consequences when asked how the data breach would impact themselves, but when asked how it would impact others, started reasoning what consequences would happen to someone else suffering from a similar data breach. As one participant noted:

> "Some might freak out" (P53)

In these cases, participants generated consequences that they only attributed in case the data breach were to happen to someone else.

. . . like their dog being stolen.

Some participants noted especially theft of dogs, whether simply raising the issue as P32 did, noting that such data breaches,

> "Make it easier for people who steal dogs to find them." (P32)

While other participants reflected in more detail about *how* theft would be enabled by the leaked data, realizing that the activity patterns could be used to infer when and where dogs were (without yet making the jump that this could also be used to reason about where *they* are):

> "I suppose it might be possible to figure out when dogs are spending time at a daycare or being boarded, which might be useful if someone wanted to harm or steal a dog. But that would still require some kind of location data." (P40)

. . . or their house being broken into.
Burglary was noted by several participants as a potential consequence for other people whose dog activity data has leaked. Some participants reasoned that the data could be used to better understand the reality on the ground, that is, what kind of dog, and how it would impact their risk assessment of breaking into the house:

> "People may be more susceptible to a home robbery if the robber knows if and what type of dog someone has. It makes it so the robber can more accurately plan for a dog presence ." (P3)

While other people reasoned more abstractly about the potential for malicious actors to observe their routine, enabling the potential for more informed burglary:

> "I suppose if activity data is leaked, people would know when you were regularly out of the house with your dog and you could be robbed...? But it's a stretch, especially considering my daily schedule changes." (P13)

. . . or (cyber) stalkers bothering them.
Some participants expanded the scope of reasoning to additional data breaching, talking in particular of the device's journal function which allows for uploading and storing of photos. Some participants spoke more abstractly in security concepts about illegal use, when photos are used without authorization, not necessarily indicating malicious use. For example, the photos being used as stock material in marketing:

> "I could see this as a concern if a person is constantly updating the journal with photos and etc. Maybe a picture might be used illegally without one's authorization but as I previously mention, not much of one's personal data would be provided with a data breach." (P39)

Additionally, participants raised worries on an abstract level of the potential implications of photo materials becoming public, noting others, rather than themselves could be worried about sensitive materials being shared:

> "if people are posting pictures of themselves or family in their journals they may be worried about those photos getting shared." (P58)

Consequences for me
Finally, we found a diverse type of potential consequences perceived by participants relating to themselves.

. . . not sure what, but it'd be bad.
Many participants expressed a negative emotional response, but could not verbalize in more details what exactly would happen:

> "Would be uncomfortable" (P41)
> "I'd be upset" (P20)

In some cases, participants expressed negative emotional responses that would cause them to reconsider use of the device – even though they were not able to verbalize exactly what would have to happen for them to decide so:

> "I really don't know...unsure if I would continue using [device brand] or not." (P46)

. . . like people finding out my routine.
Several participants focused on the precursor to other negative consequences; that others could observe their routines. In particular, the ability for this data to allow deduction of when they walk dogs and when they leave their house worried some participants:

> "Unsafe for my dog and myself. People who would want my dog or to follow me would know when I walk and for how long. They could also rob my house easily at this time as my dog and I are away." (P43)

Indeed, some participants noted clearly that this data allows for building up a detailed understanding of someone's schedule, which can be used to infer when their house or office is likely left unattended, allowing for further negative consequences:

> "It would be knowing our work schedule, when he is isn't likely to be in the house. It would offer a target to being burgled I'd think." (P61)

. . . or my location.
A component of many other worries, location was a part of the mental model of several participants while reasoning about whether consequences existed on the one hand, and whether they would be dire on the other hand. For example, some participants reasoned as above about the worry of pet theft, but discounted this because of the understanding that no exact location data is captured by the device's activity tracking itself:

> "As there is no data about where we exactly live and therefore no one could come to steal her, it would not affect us very much." (P56)

. . . and what about the rest of my digital life?
A more general notion expressed by many participants was the impact of the data breach on their *digital life*: how this data becoming public may impact their behavior and feelings in other digital services. People reasoned about the interconnectedness of the service, from having their personal data stored in the related apps. Given that several pet activity trackers now offer capability to link with their owner's regular activity trackers (e.g., FitBits), these worries relate to serious potential consequences.

> "Having access to not just our dogs data but any other personal information on our profile" (P47)
> "I would be concerned as personal information such as email address and name could be released along with information regarding each of my dogs. Hackers and identity thieves could use this information whereas dog thieves could use information on my dogs and where I take them to potentially mark them as targets." (P21)

To actual consequences of this data breach were it used maliciously, such as being spammed with e.g., dog products:

> "I don't think it would affect me badly in any way. Maybe some unwanted solicitation." (P14)

Or more sinister, the use of this data to forge information expected from the service, used for e.g., (spear)phishing:

> "I would worry about fraudulent emails perhaps posing as a weekly report." (P17)

Finally, participants noted their general worry driven by a perception of ever-present data breaches reported in the media, seemingly mediating their sense of what consequences could occur:

> "data breaches are always a concern. What a criminal can do with information is unlimited these days . It does make it difficult to participate . I get multiple phony calls a day as well as fake email" (P45)

DISCUSSION

How do the findings answer the RQs?

RQ1. What privacy concerns do dog owners perceive for pet activity data?

While noting that the focus of elicited concerns, if any, lies more with safety than privacy, the key actual *privacy* concern expressed by dog owners seems to be the ability of these devices to reveal their routine. In effect, our participants are most concerned with their ability to guarantee their own physical privacy – being able to hide from others – being impaired. Interestingly, this seems to indicate that dog owners, even when finally considering privacy, still seem to skew towards the physical aspects in their mental models. Section 5.3 will explore this in more detail.

RQ2. Are there any predictive indicators for the appearance of such privacy concerns?

None of the hypothesized indicators for the appearance of perceived privacy concerns manifested in the study, as shown in Table 2. The quantitative findings, instead, indicated a correlation between whether the device's manufacturer was perceived as trustworthy, as well as whether the use of the device was perceived to be beneficial to society as a whole. Cognitive dissonance [16] may prove a useful theoretical framing to understand these results. When facts conflict with held beliefs, people will rationalize in a way to solve this contradiction. Thus, people using these devices while holding concerns may rationalize that their greater benefit to society accounts for using the device despite having these concerns. Similarly, those using the device while holding concerns about it may rationalize their use by showing increased trust in the device manufacturer's capability to minimize relevant risks.

RQ3. What explanations underlie the extent and type of privacy concerns expressed about pet activity data?

There are several factors that explain both the (small) extent and the various types of privacy concerns expressed by participants. As the qualitative findings showed, many participants expressed no concerns, or displayed some kind of optimism bias in relegating such concerns to "others" using these devices. We posit that a key explanation here is the focus of participants on safety and physical privacy, allowing them to forego reasoning about the sensitivity of this data, mediated by illusory superiority (i.e., the Dunning-Kruger effect [24]) of their knowledge of dog behavior. In effect, they underestimate the potential information that can be inferred from the pet activity data – whether deriving detailed behavioral states using classifiers [25], inferring health statistics of their dog and themselves, or even assessing to what extent their caregiving is in line with established standards.

Service providers, on the other hand, understand the value of this data. Compare, for example, a consortium led by one pet wearable manufacturer, setting out their vision of a pet data-driven ecosystem [31] where such data is made available to e.g., veterinarians, pet hospitals, food companies, pharmaceutical companies, supplement companies, retail, service providers, research institutes, and many other types of organizations. As a result, dog owners may find themselves on the wrong side of an information asymmetry, with little understanding of the potential privacy implications this data holds. Section 5.4 will explore these implications in more detail.

How do the findings relate to other work?

In line with the findings of Zou et al. [49] on consumer risk perceptions post data-breach, we found clear optimism bias among our participants. The dog owners in our study were, when pressed for consequences, seemingly more creative in coming up with potential consequences when attributing them to others rather than themselves – including quite severe safety consequences. This may serve as an insight for further studies, that in order to elicit consequences to data breaches from participants, priming them to consider what may happen to others would likely increase the extent and possibly the variety of consequences elicited.

Where our study is not in line with other work is the extent to which users understand risks of data breaches – as found e.g., by Karunakaran et al. [22] in their large-scale study of users' views towards data breaches. This likely indicates a domain difference, dog activity trackers being perceived as innocuous technology, that malicious actors have no possible interest in. As P40 noted: "I don't see what nefarious purpose sharing dog activity data could serve. This seems like a far-fetched scenario." This indicates the need to ensure consumers understand the full extent of privacy implications the data captured by these devices hold as discussed in Section 5.4, so that they can make informed choices about the extent of privacy preserving measures they would want to take.

Besides domain effects, another explanation why so little privacy consequences are perceived can be found in the work of Zeng et al. explaining the gaps in consumers' threat models of smart homes arising due to a lack of technical knowledge [47]. Similarly, here, we would posit that a lack of dog behavior knowledge among general dog owners leads to gaps in their threat models, exacerbated by how they assess their level of dog knowledge far higher than what research and veterinary practice shows to be the case (cf. [23, 38, 46]). Additionally, Rader and Slaker found that when data capturing and processing is perceived to be transparent – highly so in this study, consumers are likely to believe no harm will come [32], further contributing to the under-estimation of privacy concerns by dog owners.

Why does safety seem to trump privacy?

When participants could come up with negative consequences, these tended to revolve around *physical safety consequences* in the real-world: dogs being stolen, houses being burgled. Consider for example P9's mention of "Invasion of privacy, insight into my daily routine - when I'm most likely with Roscoe v when I'm alone" – even though an invasion of privacy is mentioned, the perceived consequences that participants talk of are about safety. This could be explained because we are simply more attuned to think about our physical safety – certainly from an evolutionary point of view (cf. reviews of human threat management's origins [28]).

These fears are not entirely unwarranted, as for example in the UK dog theft is becoming increasingly prevalent, with an average of five dogs being stolen per week across the UK in 2017 [13]. The Blue Cross' Freedom of Information requests to UK law enforcement showed reported dog thefts increased from ± 1500 to nearly 1800 from 2013 to 2016, nearly all thefts reported as having occurred from within the owner's house. The American Kennel Club similarly reports that dog theft in the USA is on the rise [3], and cautions dog owners to be cautious with information, especially "if strangers approach you to admire your dog during walks, don't answer questions about how much the dog cost or give details about where you live." Popular media and news reports far less frequently, if at all, on potential privacy implications for dog owners using these devices, making it important to ensure consumers are educated on these matters.

Yet, for all of this seeming focus on safety, on multiple occasions people have described ways to infringe others' privacy – albeit for morally defensible reasons. For example, a novel use of dog activity trackers is "to keep dog-sitters honest" [44], discussions of which are easily found on social media groups where dog owners share their experiences with dog-sitters. To make sure their dogs are taken care of properly when left with a third party, these activity trackers allow them to verify whether their dog received the care (i.e., physical activity) they paid for, and confront dog-sitters if the observed data shows otherwise. These uses are clearly defensible from a consumer's point of view, and may only contribute positively to both dog and owner's wellbeing.

But the concern here is, that while this behavior is clearly understood as indirectly observing a third party, and deriving information about their actions, consumers do not make the leap that other, more malicious parties, may do the same to them. The lack of this leap in reasoning may explain why dog owners do not yet see privacy concerns, and provides clear paths in which to inform and explain to consumers the potential consequences by showing how well-intended use of these familiar devices may be used against them.

Why should consumers care more about dog activity data?

Because your dog's data reveals data about you...
As the qualitative findings showed, participants worry only to some extent about the possibility of their dog's activity data revealing information about them. This focused primarily on the notion of revealing routine, such as matching up spikes in activity between dog and owner to detect when someone typically leaves their house and comes back. While this is certainly to be considered in protecting dog's activity data, there is perhaps more significant information which can be inferred – related to the owner's health.

There is a clear link between dog health and human health. Dog ownership has been shown to be correlated with significant decrease in minor health problems [35] and doctor visits [36]. A study with 45 women showed marked reduction in stress response when a dog was present, as compared to when no dog was present [2], and pet ownership in general is linked to social capital and civic engagement [43] – other indicators of socio-economic status linked to health. Or quite directly: people who walk their dogs have been found to be 2.5 times more likely to reach a healthy level of moderate-intensity physical activity [37]. The bond between dogs and their owners, thus, understandably, has been positioned as a key health factor:

> "Preserving the bond between people and their animals, like encouraging good nutrition and exercise, appears to be in the best interest of those concerned with public health." [7]

Why is this an issue? Consider, for example, a recently developed model to aid in pricing health and life insurance using data from wearables [26]. Its classification of insurance-relevant health metrics includes activity measurements such as *physical activity*, with a given minimum threshold of $\geq$ 120 minutes/week leisure time exercise, and *walking duration*, with a given minimum threshold of walking $>$ 20 minutes/day.

These metrics are proposed as part of a 'health score', then used to assess risk (and subsequently, premiums) of insuring someone. In effect, dog activity data thus will likely allow for the deduction of whether the relevant thresholds have been met, and is valuable, sensitive data for those very reasons. We can infer someone is not likely to have achieved the expected threshold, made all the easier by increasing integration between dog and human activity trackers displaying shared activity patterns.

If consumers are not aware of the data's ability to reveal such information about them, there is an information asymmetry [20] between them and the service provider, who may gain advantage by selling this data, which consumers mistakenly perceive as harmless, to third parties such as insurance agents (cf [48]). The pet driven data ecosystem mentioned in Sec. 5.1 is not the only indication that this data aggregation is already happening. For example, the Mars Petcare veterinary health group recently incorporated a popular dog activity tracker, adding it to its portfolio of pet nutrition, health care, and insurance companies[2]. Telecom providers such as Vodafone have incorporated dog activity trackers into their range of devices to manage "every part of your life" with one app[3].

These ecosystems also further complicate policy matters, as it muddles even further the question of whether legislation such as the Health Insurance Portability and Accountability Act (HIPAA) applies. In 'normal' use of wearables, even though a device would capture health data, HIPPA does not apply because it only addresses "covered entities" such as health care providers, rather than personal use [29]. What though, when the use of such a wearable becomes integrated in a larger product ecosystem incorporating health services, such as e.g., data being processed to generate automated warnings to visit a veterinarian?

...and your dog's data reveals data about your caregiving.
The metrics discussed above do more than 'just' reveal data about a dog's owner – they reveal to some extent the level of care they give to their dog. Minimum standards of pet caregiving have been codified into law in several countries, making a pet owner's duty of care more than just a moral

[2] See: http://www.mars.com/global/brands/petcare
[3] See: http://www.vodafone.co.uk/v-by-vodafone/

obligation. For example, in the UK, the Animal Welfare Act (2006) enshrines the duty of a person responsible for an animal to ensure their welfare. It sets out key needs of an animal to be met, including *its need to be able to exhibit normal behaviour patterns* and *its need to be protected from pain, suffering, injury and disease*.

The UK Government published a code of practice [12] to provide dog owners with practical guidance for complying with those requirements, including advice for things that a dog activity tracker captures, such as "ensure that your dog can rest undisturbed when it wants to," and "give your dog the exercise it needs, at least daily unless your vet recommends otherwise, to keep your dog fit, active and stimulated."

A pet owner not meeting, or taking reasonable steps to ensure those needs are met would be committing an offence. Consider the *emphasized* needs in the above list – both may be potentially informed by data captured by a dog's activity tracker, whether by direct assessment of the data (e.g., do activity patterns indicate established normal activity levels), or indirectly by using classifiers to interpret data to assess its behavioral state (e.g., do activity patterns indicate any negative emotional states [25]).

The US does not have a direct analog act on a federal level, as its Animal Welfare Act (AWA) does not cover duty of care of private pet owners to their pets. Most recently, H.R. 909, or the Pet and Women Safety (PAWS) Act[4], which came into force on December 20th, 2018 effectively making it a crime to threaten someone's pet in a domestic violence situation. Such information could be derived through classifier analysis of the activity tracking data, by e.g., showing that the dog's activity can be classified as being in a fearful state. Yet, this act is limited to a very specific situation, and does not provide in general for minimum standards for duty of care that pet owners have to meet. Instead, we need to look at individual state law to assess what duty of care exists for pet owners. State animal anti-cruelty statutes provide some relevant provisions. For example, forty-four states have provisions allowing a judge to order the seizure of animals being cruelly treated or neglected [17]. California Penal Code §597f(a) similarly sets out misdemeanors for any pet owners who leave their pets without "proper care and attention." [18] The State of Pennsylvania through 18 Pa.C.S.A. §5536 regulates the "Tethering of unattended dogs." Depending on the interpretation of key terms like 'proper', whether such provisions are met can be evidenced by analyzing the data from a dog's activity tracker.

We are not claiming that it is bad *per se* that these activity trackers store a record which may have legal implications in the defense of a pet's wellbeing. Animal welfare charities such as PETA[5] and the RSPCA[6], for example, could see value in such data in their enforcement of companion an animal welfare, as would pet owners in defending against allegations of failure to meet the needs of their pet. Moreover, consider the use of dog-sitters and kennels. One popular activity tracker shows consumers the potential use of the device for monitoring how well their dog is cared for by their dog walker or at daycare. This increases transparency, indeed, but as shown above, may also carry with it legal implications that need to be considered. Should dog walking service providers be informed they are monitored with a device capturing data assessing they meet legally required minimum duty of care – and if so, would they have the right to refuse service to a dog wearing such a device?

It is thus important that the sensitive nature of this data is adequately understood both by consumer and producer of dog activity trackers, so that its potential use is known, and service providers are required to take adequate measures to protect data by ensuring the security of its storage and processing (as enshrined in e.g., the GDPR's Art. 32 or the California Consumer Privacy Act (CCPA)'s §1798.81.5).

CONCLUSION

In this paper we investigated the privacy concerns held by dog owners towards the data captured by their dog's activity tracker. We showed that many dog owners hold little concerns when presented with the scenario of a data breach leaking their dog's activity data. Where concerns do become apparent, these tend to center more on the *safety* of their dog and themselves, rather than any privacy concerns. Moreover, participants expressed several of these concerns when reasoning about other users of such devices, rather than when thinking about themselves, indicating an optimism bias.

We found only two statistically significant indicators which correlate with whether dog owners hold any concerns to this data: the extent to which they perceive the device manufacturer to be trustworthy, and the extent to which they perceive the use of the device to be beneficial to society as a whole. We posited that a key explanation for the extent and type of concerns is dog owners' focus on physical safety, perhaps driven by established media attention for e.g., dog theft. Moreover, their high self-assessed level of dog behavior knowledge, known from literature to be unlikely to translate to actual knowledge, may further lead them to under-estimate the privacy implications of dog activity data and the information that can be inferred from it such as metrics of their own health and their level of care-giving.

In addition, we discussed that, while dog owners are not seemingly concerned with privacy concerns, or indeed, perceive much value to the data these devices capture, producers and service providers of dog activity trackers *do* seem to see value in it. The integration of dog activity trackers into wider data and business ecosystems, where it is valued for third parties such as veterinarians, insurance companies, and pet service providers, means that dog owners stand, as of yet, on the wrong side of an information asymmetry. We propose that it is important to bring this discussion into the open, to inform dog owners of the value and potential privacy implications of the data captured by these devices, and to stimulate a more critical look at the extent to which privacy legislation accordingly protects it.

[4] https://www.congress.gov/bill/115th-congress/house-bill/909/text

[5] People for the Ethical Treatment of Animals – https://www.peta.org/

[6] Royal Society for the Prevention of Cruelty to Animals – https://www.rspca.org.uk/

REFERENCES

1. Ali Siddiq Alhakami and Paul Slovic. 1994. A psychological study of the inverse relationship between perceived risk and perceived benefit. *Risk Analysis* 14, 6 (1994), 1085–1096.

2. David T Allen. 1997. Effects of dogs on human health. *Journal of the American Veterinary Medical Association (USA)* (1997).

3. American Kennel Club. 2019. Protect Your Pet from Theft. `https://www.akc.org/press-center/articles/pet-theft/`. (2019). Online; accessed 30 January 2019.

4. Julio Angulo and Martin Ortlieb. 2015. "WTH..!?!" Experiences, reactions, and expectations related to online privacy panic situations. In *Symposium on Usable Privacy and Security (SOUPS)*.

5. Annie I Antón, Julia B Earp, and Jessica D Young. 2010. How internet users' privacy concerns have evolved since 2002. *IEEE Security & Privacy* 8, 1 (2010).

6. Alan M Beck and Aaron H Katcher. 2003. Future directions in human-animal bond research. *American Behavioral Scientist* 47, 1 (2003), 79–93.

7. Alan M Beck and N Marshall Meyers. 1996. Health enhancement and companion animal ownership. *Annual Review of Public Health* 17, 1 (1996), 247–257.

8. Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101.

9. Karen J Coleman, Dori E Rosenberg, Terry L Conway, James F Sallis, Brian E Saelens, Lawrence D Frank, and Kelli Cain. 2008. Physical activity, weight status, and neighborhood characteristics of dog walkers. *Preventive Medicine* 47, 3 (2008), 309–312.

10. Credence Research. 2017. Pet Wearables Market By Technology (GPS, RFID, Sensors), By Product (Smart Tags, Smart Collars, Smart Vests) - Growth, Future Prospects, And Competitive Analysis, 2017–2025. `http://www.credenceresearch.com/report/pet-wearables-market`. (2017). Online; accessed 21 February 2019.

11. Hayley Cutt, Billie Giles-Corti, Matthew Knuiman, and Valerie Burke. 2007. Dog ownership, health and physical activity: a critical review of the literature. *Health & Place* 13, 1 (2007), 261–272.

12. Department for Environment, Food & Rural Affairs (DEFRA). 2018. Code of practice for the welfare of dogs. `https://www.gov.uk/government/publications/code-of-practice-for-the-welfare-of-dogs`. (2018). Online; accessed 20 January 2019.

13. Direct Line Group. 2018. DOG THEFT CONTINUES TO RISE. `https://www.directlinegroup.com/media/news/brand/2018/20180524.aspx`. (2018). Online; accessed 30 January 2019.

14. Julia Brande Earp, Annie I Antón, Lynda Aiman-Smith, and William H Stufflebeam. 2005. Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management* 52, 2 (2005), 227–237.

15. Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Henry Dixon. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *CHI 2019*. ACM. DOI: `http://dx.doi.org/10.1145/3290605.3300764`

16. Leon Festinger. 1957. *A theory of cognitive dissonance*. Vol. 2. Stanford university press.

17. Pamela D Frasch, Stephan K Otto, Kristen M Olsen, and Paul A Ernest. 1999. State animal anti-cruelty statutes: An overview. *Animal L.* 5 (1999), 69.

18. Susan J Hankin. 2010. What is the Scope of the Duty to Provide Veterinary Care? *Maryland Bar Journal* 43 (2010). Issue 18.

19. Adam M Houser and Matthew L Bolton. 2017. Formal mental models for inclusive privacy and security. In *Symposium on Usable Privacy and Security (SOUPS)*.

20. Xiaodong Jiang, Jason I Hong, and James A Landay. 2002. Approximate information flows: Socially-based modeling of privacy in ubiquitous computing. In *International Conference on Ubiquitous Computing*. Springer, 176–193.

21. Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association Berkeley, CA, 39–52.

22. Sowmya Karunakaran, Kurt Thomas, Elie Bursztein, and Oxana Comanescu. 2018. Data breaches: user comprehension, expectations, and concerns with handling exposed data. In *Symposium on Usable Privacy and Security (SOUPS)*. 217–234.

23. Keven J Kerswell, Pauleen J Bennett, Kym L Butler, and Paul H Hemsworth. 2009. Self-reported comprehension ratings of dog behavior by puppy owners. *Anthrozoös* 22, 2 (2009), 183–193.

24. Justin Kruger and David Dunning. 1999. Unskilled and unaware of it: how difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of Personality and Social Psychology* 77, 6 (1999), 1121.

25. Cassim Ladha, Nils Hammerla, Emma Hughes, Patrick Olivier, and Thomas Ploetz. 2013. Dog's life: wearable activity recognition for dogs. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 415–418.

26. Michael McCrea and Mark Farrell. 2018. A Conceptual Model for Pricing Health and Life Insurance Using Wearable Technology. *Risk Management and Insurance Review* 21, 3 (2018), 389–411.

27. Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an IoT World. In *Symposium on Usable Privacy and Security (SOUPS)*.

28. Steven L Neuberg, Douglas T Kenrick, and Mark Schaller. 2011. Human threat management systems: Self-protection and disease avoidance. *Neuroscience & Biobehavioral Reviews* 35, 4 (2011), 1042–1051.

29. Timothy Newman and Jennifer Kreick. 2015. The Impact of HIPAA (and Other Federal Law) on Wearable Technology. *SMU Sci. & Tech. L. Rev.* 18 (2015), 429.

30. Paul A Pavlou and Mendel Fygenson. 2006. Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly* (2006), 115–143.

31. PetCommunity. 2018. PetCommunity Whitepaper v2.5. `https://petcommunity.com/PetCommunity_WhitePaper_v10.pdf`. (2018). Online; accessed 02 February 2019.

32. Emilee Rader and Janine Slaker. 2017. The importance of visibility for folk theories of sensor data. In *Symposium on Usable Privacy and Security (SOUPS)*.

33. Emilee J Rader. 2014. Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google.. In *SOUPS*, Vol. 14. 51–67.

34. Yasmeen Rashidi, Tousif Ahmed, Felicia Patel, Emily Fath, Apu Kapadia, Christena Nippert-Eng, and Norman Makoto Su. 2018. "You don't want to be the next meme": College Students' Workarounds to Manage Privacy in the Era of Pervasive Photography. In *Symposium on Usable Privacy and Security (SOUPS)*. 143–157.

35. James Serpell. 1991. Beneficial effects of pet ownership on some aspects of human health and behaviour. *Journal of the Royal Society of Medicine* 84, 12 (1991), 717–720.

36. Judith M Siegel. 1990. Stressful life events and use of physician services among the elderly: The moderating role of pet ownership. *Journal of Personality and Social Psychology* 58, 6 (1990), 1081.

37. Jesus Soares, Jacqueline N Epping, Chantelle J Owens, David R Brown, Tina J Lankford, Eduardo J Simoes, and Carl J Caspersen. 2015. Odds of getting adequate physical activity by dog walking. *Journal of Physical Activity and Health* 12, 6 Suppl 1 (2015), S102–S109.

38. Gabriella Tami and Anne Gallagher. 2009. Description of the behaviour of domestic dog (Canis familiaris) by experienced and inexperienced people. *Applied Animal Behaviour Science* 120, 3-4 (2009), 159–169.

39. Roman Unuchek and Roland Sako. 2018. I know where your pet is. `https://securelist.com/i-know-where-your-pet-is/85600/`. (2018). Online; accessed 15 January 2019.

40. Heli Väätäjä, Päivi Majaranta, Poika Isokoski, Yulia Gizatdinova, Miiamaaria V Kujala, Sanni Somppi, Antti Vehkaoja, Outi Vainio, Oskar Juhlin, Mikko Ruohonen, and others. 2018. Happy dogs and happy owners: using dog activity monitoring technology in everyday life. In *Proceedings of the Fifth International Conference on Animal-Computer Interaction*. ACM, 9.

41. Dirk van der Linden and others. 2018. Buddy's wearable is not your buddy: privacy implications of pet wearables. *IEEE Security and Privacy* 17, 3 (2018). doi 10.1109/MSEC.2018.2888783.

42. Carri Westgarth, Robert M Christley, Garry Marvin, and Elizabeth Perkins. 2017. I walk my dog because it makes me happy: a qualitative study to understand why dogs motivate walking and improved health. *International Journal of Environmental Research and Public Health* 14, 8 (2017), 936.

43. Lisa Wood, Billie Giles-Corti, and Max Bulsara. 2005. The pet connection: Pets as a conduit for social capital? *Social Science & Medicine* 61, 6 (2005), 1159–1173.

44. Zamansky and others. 2018. Log my dog – Perceived impact of canine activity tracking. *IEEE Computer* 52, 9 (2018). doi 10.1109/MC.2018.2889637.

45. Anna Zamansky and Dirk van der Linden. 2018. Activity Trackers for Raising Guide Dogs: Challenges and Opportunities. *IEEE Technology and Society Magazine* 37, 4 (2018), 62–69.

46. Anna Zamansky, Dirk van der Linden, Sofya Baskin, and Vitaliya Kononova. 2017. Is My Dog Playing Tablet Games?: Exploring Human Perceptions of Dog-Tablet Interactions. In *Symposium on Computer-Human Interaction in Play*. ACM, 477–484.

47. Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security & privacy concerns with smart homes. In *Symposium on Usable Privacy and Security (SOUPS)*.

48. Yuan-Ting Zhang, YS Yan, and Carmen CY Poon. 2007. Some perspectives on affordable healthcare systems in China. In *Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE*. IEEE, 6154–6154.

49. Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. 2018. "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association.