Privacy labels should go to the dogs

JAMES MCPARLAN, Northumbria University, UK
DIRK VAN DER LINDEN, Northumbria University, UK

Data privacy is a complex multi-faceted concept which is not easy to get a grip on, even more so when it's about you and your dog. Modern data-driven tech often has long and unreadable privacy policies making it difficult for consumers to understand what is being captured—and technology for dogs is no exception to that. Privacy labels present an alternative approach to informing consumers, aiming to provide a clear, visual summary of relevant data privacy concerns. However, no labels tailored to technology for dogs, let alone animals, seem to exist as of yet. In this work, we present an initial set of informative privacy labels usable in different contexts that inform dog owners of the most important privacy considerations for them and their dogs. The label design is grounded in the results of a mixed-method study eliciting requirements from dog owners towards typical pet technologies' data handling, cross-referenced with analysis of actual dog tech's data handling. We discuss the design of the labels, who could and should use them, and the additional uses that such labels may have for human-dog relationships.

CCS Concepts: • **Human-centered computing → HCI theory, concepts and models**.

Additional Key Words and Phrases: animal-computer interaction, pet wearable, privacy label, dog

ACM Reference Format:
James McParlan and Dirk van der Linden. 2021. Privacy labels should go to the dogs. In *ACI'21: Eigth International Conference on Animal-Computer Interaction, November 10–12, 2021, Bloomington, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The number and types of digital technologies available for our pets is ever increasing. From activity and health trackers to smart toys, auto-feeders, training apps, or even 'surveillance' cameras, this proliferation of pet technology, or 'pet tech' comes with the massive growth of how much money we spend on our pets–in the UK alone, spending reached a record high of £6.9bn in 2019 (an increase of roughly £4.14bn since 2005 [25]), while in the US spending reached $103.6bn in 2020 [2]. With the recent COVID-19 pandemic relegating not just ourselves, but our pets to our homes as well [35], the time we spend with our companion animals has increased as well. As a result, this may see a rise in adoption of pet tech as consumers become more aware of their potential caregiving benefits, seek to learn more about their pets, or simply want to have fun. Yet, little concern is typically raised about the data these technologies capturing of both the owner and dog, perhaps because people are simply not effectively informed of it. A vital component in dealing with those concerns are the privacy policies that come with data-driven pet tech, which in an ideal world would clearly and unambiguously describe how, why, and what they do with your data. But privacy policies, even if they are read, which they frequently are not [9], are often too complicated, too long, or simply too confusing [24]. Privacy labels [13] on the other hand, visually inform relevant details that might otherwise be lost through complex policies.

While Animal-Computer Interaction (ACI) research has explored the privacy policies of some types of pet tech [34] and the privacy concerns that people may have as a result [32, 33], little practical work has yet been done proposing design artifacts to inform and educate consumers who use such technology. Dogs, in particular, are an important topic of research in this context as their close link to their human caregivers hold strong privacy implications (and concerns) [34] beyond that of other pets [32]. This article contributes to the growing body of ACI research on managing privacy in human-animal-technology triads by providing an initial foray into:

(1) **Determining the requirements for pet tech privacy labels** focusing in particular on technology for dogs through a mixed-method study investigating dog owners' attitudes and thoughts towards pet tech and privacy(N=69) combined with AI-driven privacy policy analysis; and
(2) **designing a set of privacy labels for pet tech** appropriate for different contexts that enable us to more effectively inform consumers of relevant data privacy considerations when considering a new pet tech device.

The rest of this article is structured as follows. Section 2 discusses relevant research on technologies for dogs, privacy (labels), and their intersection. Section 3 discusses the user study conducted to elicit requirements towards the label, whose design process and artifacts are discussed in Sections 4–5. We conclude in Section 6.

2 BACKGROUND

2.1 Dog tech (and privacy)

Pet tech is an umbrella term for the category of products and services designed to better the health and well-being of our pets [3], with 'dog tech' similarly being such products tailored towards dogs (and their human caregivers). These technologies range from software, consumer grade hardware, and even industrial grade solutions used by veterinarians and other animal professionals, frequently based around collecting and interpreting data to help inform caregivers on an animal's behavioural and/or physiological condition [3]–effectively giving rise to an 'interspecies information system' [31] where human caregivers are given processed animal data to act upon.

ACI research as a result is inherently linked to the design and development of such technology, being focused on improving our understanding of how animals live in their environments, and how we can live together better [18]. Within ACI, the focus of Dog-Computer Interaction (DCI) in particular provides important cues to understanding the importance of proper design of dog tech, whether that is for dog-human or dog-dog interactions [12]. DCI interactions effectively provide a means of interspecies data collection that can subsequently be acted upon [31], and has focused on tech such as monitoring and tracking dogs [16], training them [20], improving their working functions [23], collect information about their physiology [17], or simply playing games and having fun [5]. ACI/DCI research has shown how appropriate use of certain dog tech can help raise quality of life for dogs by giving allowing their caregivers to tailor their care and behaviour towards the dog [28, 37]. Other recent ACI research has expanded the scope of DCI to enabling human-dog interaction on more distant scale (e.g., by enabling tele-presence [14, 27], or embedding dog tech into wider social contexts such as dog parks [15].

Given the close link between humans and their pets–especially with companion animals like dogs, dog data captured by such technology will most certainly reveal information about their human owner [34]. This is further complicated when a dog lives with multiple humans, and interacts also with others, such as family friends, visitors, or veterinarians–all of whom might not take kindly to being indirectly monitored [33]. Knowing what data devices capture is thus critical to allow for informed use of pet tech. Beyond considering 'just' the human-animal dyad themselves, the increasing integration of pet tech into smart home ecosystems makes it further important to consider its myriad of privacy implications. Seemingly innocuous data gathered by smart home tech can be used to determine whether houses are empty [36], which observation of pet data would also allow for [33]. Studies on smart toys for (human) children similarly showed concerns for recording and data sharing [19], especially when involving microphones and speakers, as malicious actors could e.g., cause behavioural distress by playing disturbing noises [30]–which is similarly a threat to pet welfare with increasing smart toys for pets. Indeed, data breaches have occurred already involving pet tech allowing for tele-communication with dogs or other pets left alone at home [11].

2.2 From privacy policy to privacy labels

Research has shown that privacy policies are frequently not read [9], perhaps because they are typically difficult to read as they contain too much 'legalese' [21] and are often too complicated, long, and confusing [24]. Research has shown how most policies would require college education level to understand their syntax and semantics [1]. This frequently discourages users from reading privacy policies, and in turn makes it difficult for consumers to be truly aware of what implications using tech may have for them.

As a potential aid to this issue, privacy labels have been proposed and increasingly used. A noteworthy point for their development was the introduction of the 'food nutrition label' metaphor for privacy [13], designed to mimick such labels and visually present the most important security and privacy concerns a consumer might have. Context-dependent design has become increasingly accepted, using e.g., QR codes to link consumers to further detailed information, and using readable versions for different purposes, from extensive grid-based labels that cover most information, to simplified labels communicating only the essential [6, 7]. While initially criticism of privacy labels was that manufacturers or vendors who were not particularly privacy minded would have little incentive to include them, this has changed over the last years as platform operators such as Apple have introduced mandatory privacy labels for software in its App Store [26]. Given that most pet and dog tech is data-driven hardware controlled by an associated app, this thus makes it feasible to always have at least one context where a privacy label can be implemented, and subsequently lower the barrier for vendors to share privacy labels in other parts of their product delivery.

Importantly, privacy labels should not necessarily be seen as design artifacts that have concrete behavioral change as their end goal. Rather, privacy labels are meant to aid in reducing the information asymmetry between consumer and vendor so that they have an honest chance at *informational self-determination*–giving them not just the right, but the ability to "exercise personal control over the collection, use and disclosure of their personal information by others" [4]. As research has shown, many consumers are still happy to use technology even if it uses their data for myriad of purposes [8], which is their own right. But such decisions should be made as informed as possible, for which clear and understandable information is needed, hence the privacy label.

3 DETERMINING THE REQUIREMENTS FOR DOG TECH PRIVACY LABELS

To determine what information is most important to clearly convey in a privacy label for pet tech we conducted a mixed-method study involving a quantitative and qualitative survey of dog owners' perceptions and beliefs towards pet technologies, followed up with AI-driven analysis of commercially available pet technologies. We obtained ethics approval from our Institution's Institutional Review Board (IRB) before any empirical work began.

3.1 Study design

3.1.1 Participants. Sixty-nine dog owners were recruited through UK-focused social media networks including Twitter, Facebook, and Instagram. No personal data was recorded. All participated volunteered and received no compensation for their participation.

3.1.2 Materials. We implemented a questionnaire eliciting a mixture of binary, Likert, and qualitative open data (see Appendix A for the full instrument) with four key sections, first asking questions about participants' dogs and the relationship, followed by their experience with, and attitude towards digital technologies for dogs, their views on data collected by such devices and privacy policies, and finally their basic demographics.

3.1.3 Analysis. We analyzed the results of the questionnaire to build a codebook (see Table 1) identifying the types of dog technologies that people owned, aspects that dog owners would want to be informed about, and further privacy related attitudes: do people tend to read privacy policies, and what data do people believe dog technologies capture. Next, we used PriBot [10] to analyze the privacy policies of a cross-section of the types of dog technologies owned by people in the questionnaire, comparing how these technologies' data practices 'in the wild' compare to what dog owners believe they do, and find permissible.

3.2 Findings

3.2.1 Demographics. Sixty-nine UK citizens participated in the study (78% Female, 22% Male). In total they gave care to 89 dogs, with a fair variation in breeds (44% small, 29% medium, and 27% large breeds), with dogs' age varying between 3 month old puppies and 15 year old seniors. As could be expected with the current pandemic situation, most dogs spent most of their time in close proximity to their caregivers (18.1% all day, 58.3% most of the day, 11.1% a couple of hours per day, and only 6.9% less than an hour per day). While most (75%) of the queried participants did not yet own any technology, already a significant group (25%) actively used a typical variety of technologies, as shown Fig. 1. Interestingly, people who owned/used dog tech, predominantly lived with mature or older dogs(≥6 yrs) to use tech.

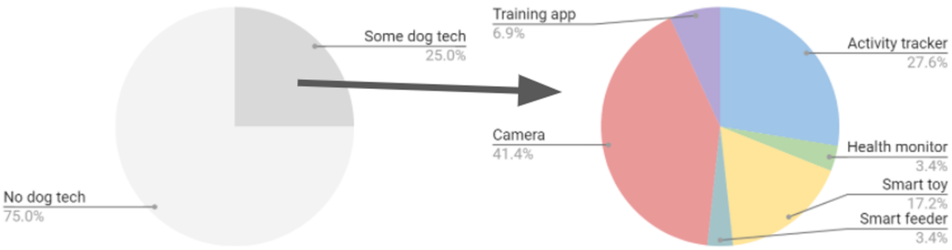


Fig. 1. Dog owners owning some type of dog tech, and the types owned

3.2.2 Privacy attitudes and beliefs. Only a minority of participants reported reading privacy policies (22%), some indicated skimming them (12%), while the rest simply did not read them at all (67%). Participants agreed that privacy policies are too complex (median=4±0.9) while nearly all participants strongly agreed that they are too long (median=5±0.6). Given these findings it is especially relevant to understand their beliefs regarding what dog tech captures, so as to contrast this with the reality of devices on the market, as shown in Fig. 2. We split up the participants into owners of dog tech and those who did not own anything to assess whether there was any difference. Fisher’s exact test showed no significant difference, regardless of whether only considering ‘yes’ (p=0.67) or ‘yes’ and ‘maybe’ together (p=1).

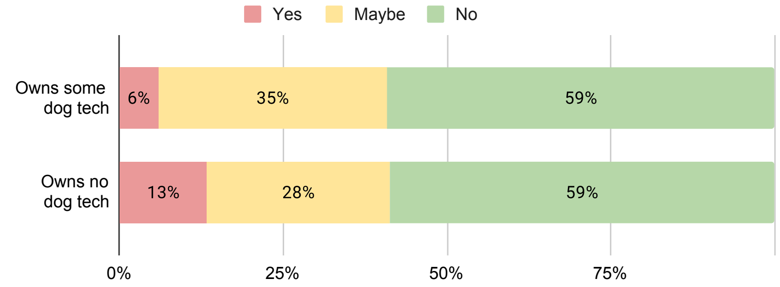


Fig. 2. Distribution of participants believing dog technologies captured data of themselves.

To further understand *what* participants want to be informed about, we conducted an inductive analysis of the qualitative data, identifying and coding relevant recurring aspects, resulting in the codebook summarized in Table 1. When asked what data participants thought dog tech would capture of them and their dog, a recurring answer was simply not knowing or being unsure–also among those who already owned and use dog tech. This was in line with most participants not reading privacy policies, and research showing that even if they were to read them, privacy policies of e.g., pet wearables are vague to the point of making it impossible to understand exactly what is captured [34].

Code	Definition	Quote(s)	Count
Data Sharing	Participants want to understand who their data is being shared with and why.	*“Not going to share my dog’s medical information or where the dog lives/ goes to the vets”*	20
Data Use	Participants want to understand why it is necessary for organisations to collect and use their data.	*“What will happen with the information they receive”*	16
Security Measures	Participants want to know what procedures are in place to keep their data safe and limit misuse.	*“That it would be secure to hackers given the large number of dog thefts. If it showed my / my dogs’ location I would be very worried. Additionally, it would show when I was out of my home when walking leaving my house vulnerable when I’m not there. Security would be key.”*	15
Type of Data	Participant finds it important to know clearly what types of data are captured.	*“All the data types collected in a clear, prominent list /.../”*	14
Data Storage Location	Participants want to know where data is stored physically and/or electronically.	*“Any collected data, how it is used, stored. Is it sold to 3rd parties?”*	11
Legislation	Participants want to know what laws protect them when they consent to a product and its policy.	*“Safety for the dog, security, data handling to GDPR legislation”*	8
Data Storage Duration	Participants want to know the length of time data is kept and stored for.	*“What is stored, who it would be shared with (specific companies- not just â€˜3rd parties’) length data is stored, how to delete it”*	5
Understandability	Participants want to be able to understand the information included in a privacy policy.	*“Easy to understand. Make their policy clear. Don’t use jargon”*	5
Data Ownership	Participants want it highlighted who owns and controls the data given to the organisation.	*“Who has ownership of the data and following that can it be sold on or used by other third-party companies for targeted marketing”*	1

Table 1. Partial codebook: Aspects identified in the qualitative analysis that participants (N=69) want to clearly know

Thus, the recurring concerns we identified through the qualitative analysis are of vital importance for determining what a privacy label should inform consumers of. In particular, the main concerns that people have are regarding data sharing (what is captured, and whom is it shared with?), data use (why is it used and shared?), and security measures in place (how is my data protected?), with further additional concerns regarding where data is stored, appropriate legal safeguards beyond technical security measures. Given the types of technologies owned by participants (cf. Fig. 1) such as cameras and activity trackers and a growing sense of societal awareness of data breaches and their potential impacts, these are understandable concerns.

3.2.3 Contrast of privacy attitudes and beliefs with dog tech data practices. Using PriBot [10], we analyzed a prototypical example of a commercially available dog tech device for the main types of dog tech owned. We then tabulated the data according to the main concerns we identified (data sharing, data use, security measures), mapping them to typical privacy policy elements such as data collection, third party sharing, consumer choice, security, and data retention. Table 2 gives an overview of what privacy policies inform consumers of in this regard, and more importantly, where they fail to clearly inform consumers of this by e.g., only mentioning 'Other Data' regarding what data is shared with third parties, or fail to provide any information regarding their choices as to what data is shared, or how long it is retained for. A privacy label design thus needs visually cover these key elements, and also clearly signal to consumers when key information is unknown.

Technology	**Data Collected**	**3rd Party Sharing**	**Your Choices**	**Security**	**Data Retention**
Camera	Contact Cookies and Tracking Demographic Location Survey Data Generic Personal Information Other Data	Computer Information Contact IP Address and Device Ids Survey Data Online Activities Generic Personal Information Other Data	First Party Use First Party Collection Third Party Sharing Collection	Generic Other Security Measures Secure Data Storage	n/a
Activity Tracker	Computer Information Contact Cookies and Tracking Demographic Health IP Address and Device ids Location Personal Identifier Social Media Data Survey Data User Online Activities User Profile Other Data	Financial Other Data	First Party Use	Generic Other Security Measures Data Access Limitation	n/a
Smart Toy	Contact Financial Survey Data	Other Data	Other Data	Data Access Limitation Other Security Measures Secure Data Transfer Privacy Security Program Secure Data Storage	n/a
Training App	Computer Information IP Address and Device ids Location Generic Personal Information User Online Activities Other Data	Financial Other Data	n/a	Other Security Measures Secure User Authentication Generic	Generic Personal Information
Health Monitor	Health	Computer Information Contact Health Other Data	First Party Use	Other Security Measures	n/a

Table 2. Privacy policy analysis of several commercially available dog technologies according to participants' requirements

4 DESIGNING PRIVACY LABELS FOR DOG TECHNOLOGIES

Following the determination of requirements for dog tech privacy labels, and taking into account prior art on privacy labels and visual design, we now develop an initial set of privacy labels for dog tech suitable for multiple contexts.

4.1 Translating requirements into design principles

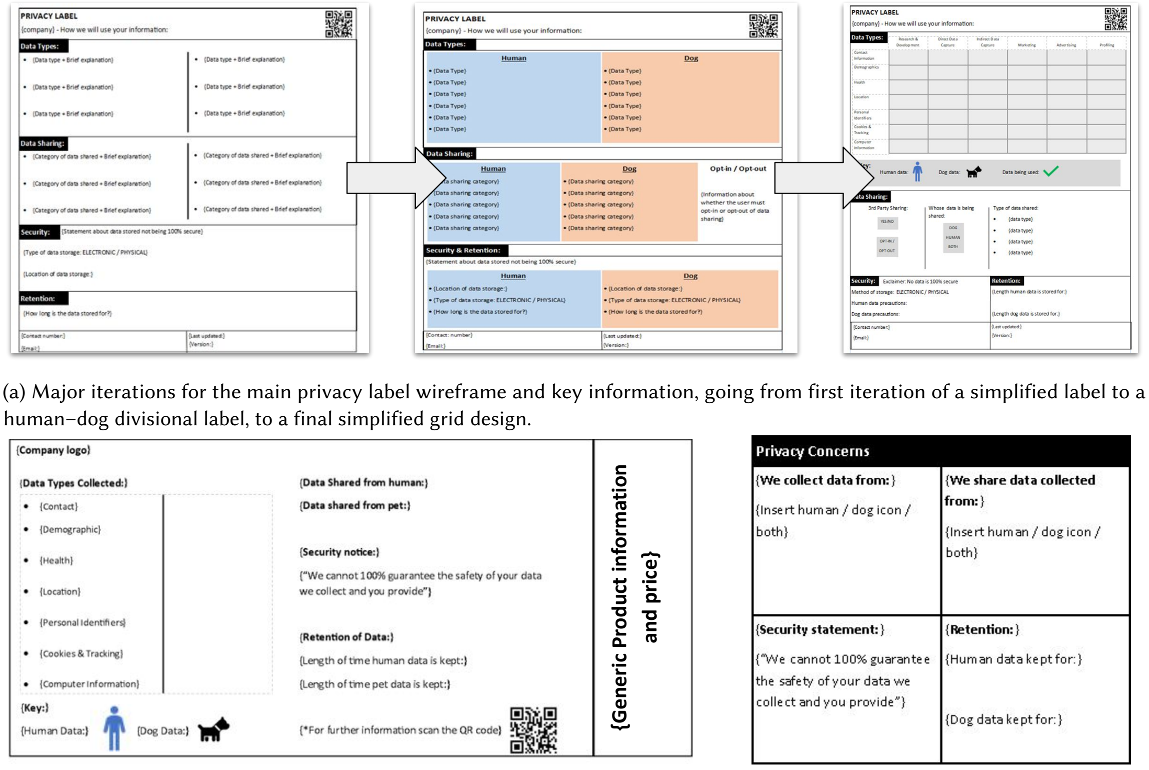
We used the insights gained from our user requirements study and took into account insights into privacy label design [13] and general principles for cognitively effective visual design [22] to distill the following critical domain-specific design principles for privacy labels of dog technologies:

- as we found that most participants did not believe dog tech captured data of themselves (see Fig. 2), *the label must explicitly show what data is captured of human and animal*
- as we found that policies are too long to read, *the label must only present the most salient information for users*, namely (as per Table 1):
  - Data collection: what types of data are captured of whom?
  - Data sharing: what and whose data is shared for what purpose under what assumption?
  - Security: where is data stored, and what precautions are taken?
  - Retention: what and whose data is kept for how long?
- as we know that different contexts have different informational affordances, *the label must show an appropriate amount of information for its purpose*, namely allowing for:
  - ...fully informing consumers of all relevant information by a full label
  - ...informing consumers of relevant details in a retail setting
  - ...briefly informing people what is collected and shared of under what security measures with minimal space
- as we know that all information needs to be available on request, *any label must link to the fullest form*
- as we know that data collection and processing can change over time, *the (full) label must clearly show the date of its privacy assessment*

4.2 Design Process

Using these principles and prior art of privacy labels as input, we iteratively constructed wireframes for the privacy label, going through several major design phases (see Fig. 3a) to produce a final full label and several additional labels covering the other contexts (see Figs 3b– 3c). Initially we created a label where information was presented straightforwardly the most important information divided into sections, and further subdivided into two columns for human and dog. We found this not offer a visually expressive enough cue to distinguish between human and animal data, so we separated the data and used dual coding with color to distinguish between the two. As this lacked semantic transparency (i.e., immediately conveying the real-world meaning), we further iterated towards a matrix form where symbols depicting human and dog directly indicate whose data is captured of (and for what purpose). In order to ensure readability and ease of translation between platforms, we specifically encoded this information with standard emojis, so that all platforms in which labels are read can easily insert their relevant designs.

To account for the other two main contexts in which labels would be used, we further designed a typical product label (Fig. 3b) incorporating product information and pricing on the right hand, with key privacy information on the left hand, using the same semantically transparent emoji approach to map whose data is captured for what. In this contexts with the label having a reduced set of information, linkage to fullest form of information was especially important,


PRIVACY LABEL
{company} - How we will use your information:
Data Types:
Data Sharing:
Security:
Retention:
Human
Dog
Opt-in / Opt-out
Security & Retention:
{Company logo}
{Data Types Collected:}
{Contact}
{Demographic}
{Health}
{Location}
{Personal Identifiers}
{Cookies & Tracking}
{Computer Information}
{Key:}
{Human Data:}
{Dog Data:}
{Data Shared from human:}
{Data shared from pet:}
{Security notice:}
{"We cannot 100% guarantee the safety of your data we collect and you provide"}
{Retention of Data:}
{Length of time human data is kept:}
{Length of time pet data is kept:}
{*For further information scan the QR code}
{Generic Product information and price}
Privacy Concerns
{We collect data from:}
{Insert human / dog icon / both}
{We share data collected from:}
{Insert human / dog icon / both}
{Security statement:}
{"We cannot 100% guarantee the safety of your data we collect and you provide"}
{Retention:}
{Human data kept for:}
{Dog data kept for:}

(a) Major iterations for the main privacy label wireframe and key information, going from first iteration of a simplified label to a human–dog divisional label, to a final simplified grid design.

(b) Additional label for retail settings

(c) Additional label for minimal space

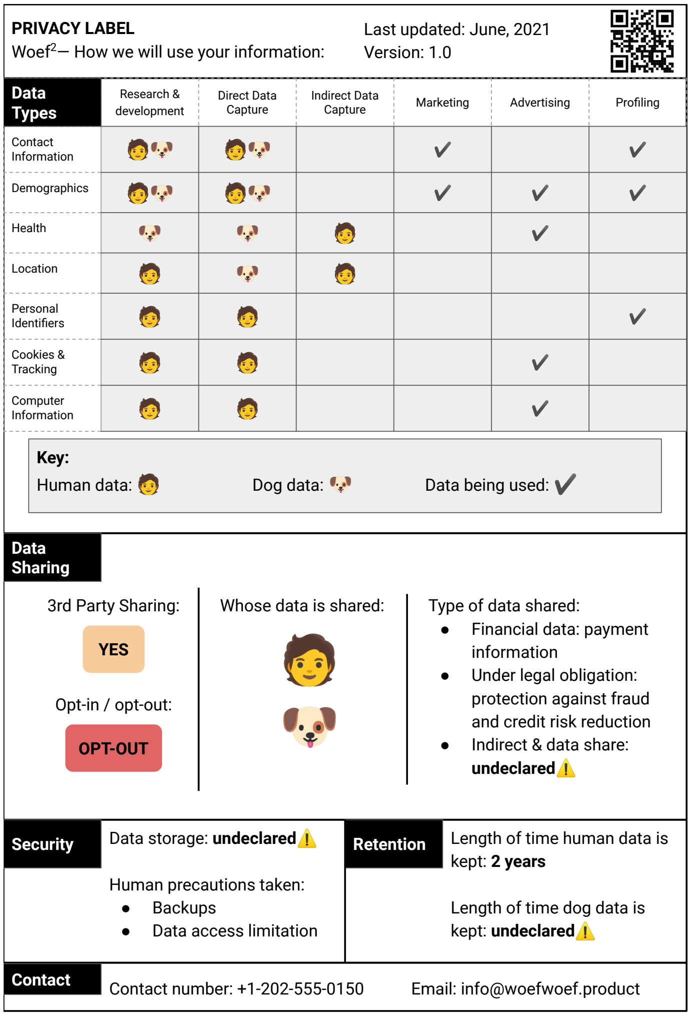
Fig. 3. Development of wireframes for privacy labels

so that a QR code was integrated into the design to allow for linking either to a digital version of the full label, or additional explanatory documents on e.g., the product websites. A second 'sticker' label (Fig. 3c) was further developed to represent only the minimal necessary information, capturing whom data is collected from and shared with under what assumptions, which can be represented either digitally (e.g., as a pop-up before installing relevant software), or physically as stickers appended to product boxes or displays.

4.3 Contextual label designs

For a more concrete example, we produced instantiations of the labels for "Woef^2", a fictional but typical product.

4.3.1 Full labels. Figures 4 shows an example of a full label, conveying all information needed to address the most important privacy-related concerns dog owners would have. The grid square in data types shows for each type of data (e.g., 'health', 'location') whether it is captured and used for a particular purpose–and of whom. This gives an immediate overview of just how much personal data typical pet tech products might capture, and make it clear to consumers that their data is used extensively, as well as visually indicating to what the device is limited in terms of helping them understand their dog. This grid distinguishes between direct and indirect data capture, showing where, due to the entangled nature of the human-dog relationship, data of a human or dog is indirectly captured through



PRIVACY LABEL
Woef^{2}— How we will use your information:

Last updated: June, 2021
Version: 1.0

Data Types	Research & development	Direct Data Capture	Indirect Data Capture	Marketing	Advertising	Profiling
Contact Information	🧑🐶	🧑🐶		✓		✓
Demographics	🧑🐶	🧑🐶		✓	✓	✓
Health	🐶	🐶	🧑		✓	
Location	🧑	🐶	🧑			
Personal Identifiers	🧑	🧑				✓
Cookies & Tracking	🧑	🧑			✓	
Computer Information	🧑	🧑			✓	

Key:
Human data: 🧑 Dog data: 🐶 Data being used: ✓

Data Sharing

3rd Party Sharing:
YES

Opt-in / opt-out:
OPT-OUT

Whose data is shared:
🧑
🐶

Type of data shared:
- Financial data: payment information
- Under legal obligation: protection against fraud and credit risk reduction
- Indirect & data share: **undeclared**⚠

Security

Data storage: **undeclared**⚠

Human precautions taken:
- Backups
- Data access limitation

Retention

Length of time human data is kept: **2 years**

Length of time dog data is kept: **undeclared**⚠

Contact

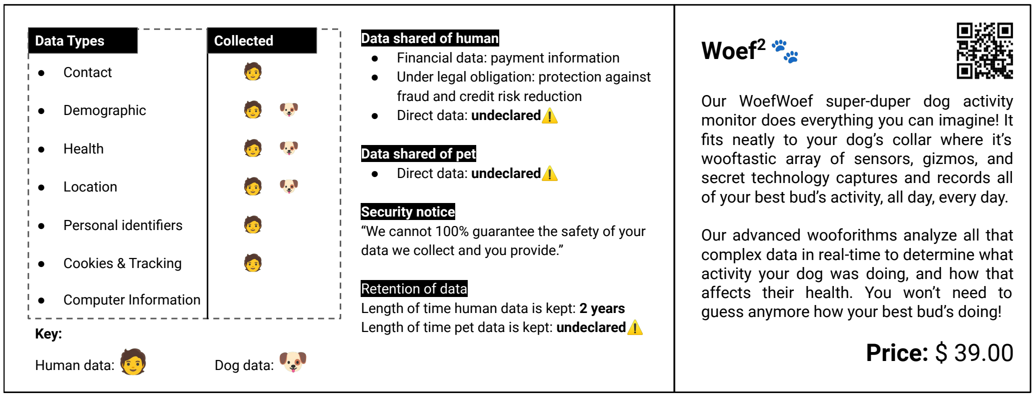
Contact number: +1-202-555-0150 Email: info@woefwoef.product

Fig. 4. Example of a full label for a fictional product.

the other. Fig. 4 indicates that Woef^{2} indirectly captures an owner's health and location data a result of direct data capture of the dog—that is, due to frequent co-location dog location becomes a proxy for owner location, and parts of dog health data such as activity similarly become partial proxies for the owner's health.

The data sharing section provides further clear visual cues for important information such as whether data is shared to third parties beyond the vendor, and whether this data is shared until the consumer does something about it ('opt-out'), or whether it only happens if they do something for it ('opt-in'). Effectively, the column showing whose data is shared serves as an additional way of visually coding that these devices do not capture only data of animals, but of human users as well. These labels could be provided physically as print-outs e.g., as part of the package should vendors be privacy-minded and/or position their products as so (an increasingly viable business case), as well as digitally as the 'full' label referred to by other more minimal versions through e.g., QR codes.

4.3.2 *Retail label.* As not all products could feasibly come with large full physical labels, or vendors could opt not to provide them, a retail-oriented label can combine product information together with the main privacy considerations relevant to dog owners. The retail label as shown in Fig. 5 accounts for this by highlighting both the relevant product details, privacy information, and linkage to further full details through e.g., QR codes. Unlike the full label, the smaller retail label does not distinguish between direct/indirect data capture, and therefore directly shows that human and dog health data are captured, even though only dog health data is captured directly.



Data Types	Collected
Contact	🧑
Demographic	🧑 🐶
Health	🧑 🐶
Location	🧑 🐶
Personal identifiers	🧑
Cookies & Tracking	🧑
Computer Information	

Key:

Human data: 🧑 Dog data: 🐶

Data shared of human

- Financial data: payment information
- Under legal obligation: protection against fraud and credit risk reduction
- Direct data: **undeclared**⚠

Data shared of pet

- Direct data: **undeclared**⚠

Security notice

"We cannot 100% guarantee the safety of your data we collect and you provide."

Retention of data

Length of time human data is kept: **2 years**
Length of time pet data is kept: **undeclared**⚠

Woef^2 🐾

Our WoefWoef super-duper dog activity monitor does everything you can imagine! It fits neatly to your dog's collar where it's wooftastic array of sensors, gizmos, and secret technology captures and records all of your best bud's activity, all day, every day.

Our advanced wooforithms analyze all that complex data in real-time to determine what activity your dog was doing, and how that affects their health. You won't need to guess anymore how your best bud's doing!

Price: $ 39.00

Fig. 5. Example of a retail label for a fictional product.

Such a label can be used by e.g., re-sellers and stores as shelf labels to further inform their customers. As an additional benefit, the use of such label would inform consumers *before* purchasing these devices, and reduce the situation of purchasing a device only to find out they disagree with its terms and conditions and having to return it.

4.3.3 *Minimal label.* Finally, a minimal label as shown in Fig. 6 can be used when there is very little physical space available, to complement physical products (e.g., by stickers appended to a product's packaging), or as an additional virtual label that consumers are shown when installing a dog tech's controlling software. These labels are by their nature designed to show only the most critical information, in particular to inform consumers just whom data is collected of and shared with, under what typical assumptions, while relying on the consumer to read further information to assess the main details.

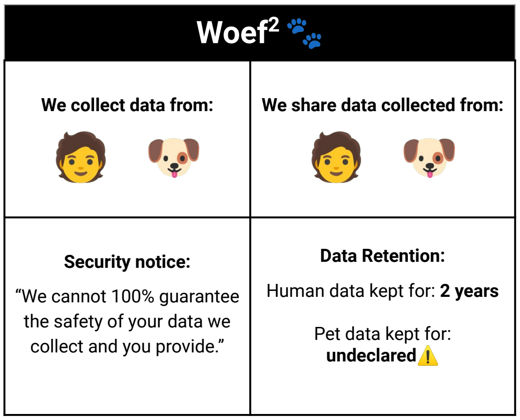
The simple design of this label is meant to convey purely the critical information to allow consumers to make a quick decision whether a product would be potentially suitable with their privacy expectations, akin to e.g., increasing use of the green tick to indicate food products are compatible with a vegetarian lifestyle.

5 DISCUSSION

While this paper has presented a requirements study and initial designs for privacy labels, further considerations and thoughts as to their deployment, and the effect they may have not just on privacy considerations but human-dog relations are things we need to tackle in further research.

5.1 Who are these labels for?

It is well known that some technology makers might not be interested at all in reducing the information asymmetry between them and their customers and thus would not adopt these labels (at least voluntarily). However, that is exactly



Woef^2 🐾

We collect data from:	We share data collected from:
🧑 🐶	🧑 🐶
Security notice: "We cannot 100% guarantee the safety of your data we collect and you provide."	**Data Retention:** Human data kept for: **2 years** Pet data kept for: **undeclared**⚠️

Fig. 6. Example of a sticker label for a fictional product.

why a variety of designs, for different purposes becomes vital. Even if a technology maker does not want to inform consumers, vendors (e.g., shops) could do so by displaying versions of the retail label (Fig. 5) on product floors, and/or putting versions of sticker labels (Fig. 6 on products.

That said, many technology makers are also increasingly realizing the growing desire for explicit informational self-determination, and the backlash against companies and products seen to infringe on this. Combine that with the move of digital platforms such as Apple's App Store displaying a kind of label for software to inform potential users of an app's privacy practices, and there seems to be more than enough potential for both physical and digital privacy labels for dog technologies to be deployed, hopefully by willing makers of these technologies in collaboration wit their vendors and software platform markets.

5.2 How should these labels communicate the complexity of 'dog-to-human' indirect data capture?

The current design iteration of the labels only explicitly communicate indirect data capture in the full label design. This requires these labels to be used, or consumers to access it through the QR code in a (smaller) variation of the label. In the more compact labels, however, in the absence of a grid of data types and purposes, while it is communicated that human data is captured, there is no mention of it being done indirectly. Instead, it is simply reduced to splitting up into saying "Health data is collected" about human and dog–which is strictly true. But this does perhaps not inform consumers clearly enough that such collection happens indirectly and is thus may be difficult to exercise informed control over.

As the indirect capture of human data through direct dog data capture is one of the major things to consider when thinking about privacy implications of such technology, it is important this is clearly conveyed. We had considered at first footnotes, but this feels counter-intuitive to a succinct, more graphical nature of labels. To thus also convey that not only human health data is also captured as in the fictional example of Woef^2, it is captured indirectly, an additional symbol for the smaller retail and sticker labels could emphasize this. An option could be, in the vein of EmojiMashupBots, to add a specialized 'entangled' human-dog symbol, such as shown in Fig. 7 using the 'person' and 'dog' emojis as rendered in some of the current dominant platforms.

However, further user research is required to ensure semantic transparency of such a symbol (i.e., clearly indicating the entangled indirect nature of data capture), that it renders well, and stays legible in different formats and platforms.

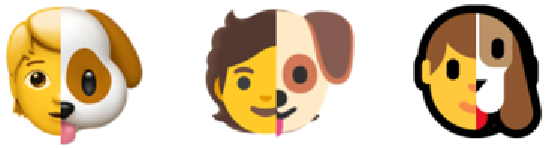


Fig. 7. Dog-human emoji mashup for dominant platforms as a potential symbol for indirect human data capture via dog.

5.3 Informing, or altering the human-dog relationship?

Beyond informing dog owners of the data that dog tech capture of them and their best friend, these labels might also further serve to inform humans of just how extensive the interspecies relationship with a companion animal becomes by confronting them with just how much of our data is intertwined, and as a result, how much of our lives are. Thus, beyond serving immediately for the benefit of the human in the human-dog dyad, they can aid in a fundamental role of technology for animals frequently addressed by ACI research [29]: improving bonding by stimulating further reflection on our roles, interspecies activities, and what is owed to each other. For example, extensions of labels beyond immediate privacy could for example, inform further of whether technology supports 'just' dogs, or the dog-human dyad for particular activities, and what aspects of their relationship and caregiving it affects on.

6 CONCLUSION

Consumers have a clear lack of interest in reading privacy policies–and most policies are not made to be read whether by human or animal, making it critical that relevant privacy information is conveyed through other means. Given the growing use of pet tech, and technology for dogs in particular ranging from cameras, trackers, toys, software and beyond, it is important that consumers know exactly what data these devices collect and share, and of whom they do so.

Based on insights gathered through a requirements study with dog owners in the UK we designed three empirically grounded privacy labels, a full, grid-based label, a retail-oriented label to accompany physical products, and a minimal label that can accompany physical products in sticker form or be a virtual label for software. We envision that further development of these labels (and their trivial adaption to other companion animals such as cats) will allow to better inform consumers of the extent of data collection and use of pet technologies, as ACI research has shown consumers are typically not aware of the scope or use cases of this, leading to a strong information asymmetry between consumer and those benefiting from their data [33].

REFERENCES

[1] Annie I Antón, Julia Brande Earp, Qingfeng He, William Stufflebeam, Davide Bolchini, and Carlos Jensen. 2004. Financial privacy policies and the need for standardization. *IEEE Security & privacy* 2, 2 (2004), 36–45.

[2] APPA. 2020. *Pet Industry Market Size, Trends & Ownership Statistics.* https://www.americanpetproducts.org/press_industrytrends.asp

[3] Barkytech. 2021. *The Ultimate Consumer Guide to Pet Technology.* https://barkytech.com/ultimate-consumer-guide-pet-technology/

[4] Ann Cavoukian. 2008. Privacy in the clouds. *Identity in the Information Society* 1, 1 (2008), 89–108.

[5] Elizabeth Cox, Clara Mancini, and Luisa Ruge. 2020. Understanding Dogs' Engagement with Interactive Games: Interaction Style, Behaviour and Personality. In *Proceedings of the Seventh International Conference on Animal-Computer Interaction.* 1–12.

[6] Lorrie Cranor. 2002. *Web privacy with P3P.* " O'Reilly Media, Inc.".

[7] Lorrie Faith Cranor, Praveen Guduru, and Manjula Arjula. 2006. User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction (TOCHI)* 13, 2 (2006), 135–178.

[8] Bernhard Debatin, Jennette P Lovejoy, Ann-Kathrin Horn, and Brittany N Hughes. 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of computer-mediated communication* 15, 1 (2009), 83–108.

[9] Susan E Gindin. 2009. Nobody reads your privacy policy or online contract: Lessons learned and questions raised by the FTC's action against Sears. *Nw. J. Tech. & Intell. Prop.* 8 (2009), 1.

[10] Hamza Harkous, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G Shin, and Karl Aberer. 2018. Polisis: Automated analysis and presentation of privacy policies using deep learning. In *27th USENIX Security Symposium (USENIX Security 18)*. 531–548.

[11] Hautala. 2017. *Smart toy flaws make hacking kids' info child's play.* https://www.cnet.com/home/smart-home/cloudpets-iot-smart-toy-flaws-hacking-kids-info-children-cybersecurity/

[12] Ilyena Hirskyj-Douglas and Andrés Lucero. 2019. On the Internet, Nobody Knows You're a Dog... Unless You're Another Dog. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

[13] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. 2009. A" nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. 1–12.

[14] Chloe Kliman-Silver. 2020. Examining The Animal-Human Bond Through The Lens Of Telepresence. In *Proceedings of the Seventh International Conference on Animal-Computer Interaction*. 1–5.

[15] K Cassie Kresnye, Alec Andrew Theisz, Lauren Trester, and Patrick C Shih. 2019. Barks & Rec: A Dog Park Socio-Technical System. In *Proceedings of the Sixth International Conference on Animal-Computer Interaction*. 1–6.

[16] 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*. 415–418.

[17] Germain Lemasson, Dominique Duhaut, and Sylvie Pesty. 2015. Dog: Can you feel it. *Animal Computer Interaction@ British Human Computer Interaction (BHCI), Lincoln, England* (2015).

[18] Clara Mancini. 2011. Animal-computer interaction: a manifesto. *interactions* 18, 4 (2011), 69–73.

[19] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys that listen: A study of parents, children, and internet-connected toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 5197–5207.

[20] Sean Mealin, Marc Foster, Katherine Walker, Sherrie Yushak, Barbara Sherman, Alper Bozkurt, and David L Roberts. 2017. Creating an evaluation system for future guide dogs: A case study of designing for both human and canine needs. In *Proceedings of the Fourth International Conference on Animal-Computer Interaction*. 1–6.

[21] George R Milne and Mary J Culnan. 2004. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of interactive marketing* 18, 3 (2004), 15–29.

[22] Daniel Moody. 2009. The "physics" of notations: toward a scientific basis for constructing visual notations in software engineering. *IEEE Transactions on software engineering* 35, 6 (2009), 756–779.

[23] Charlotte L Robinson, Clara Mancini, Janet Van Der Linden, Claire Guest, and Robert Harris. 2014. Canine-centered interface design: supporting the work of diabetes alert dogs. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 3757–3766.

[24] Manuel Rudolph, Denis Feth, and Svenja Polst. 2018. Why users ignore privacy policies–a survey and intention model for explaining user privacy behavior. In *International Conference on Human-Computer Interaction*. Springer, 587–598.

[25] Statista. 2019. *Leading pets owned by households in the United Kingdom (UK) 2019.* https://www.statista.com/statistics/308218/leading-ten-pets-ranked-by-household-ownership-in-the-united-kingdom-uk/

[26] NY Times. 2021. *What We Learned From Apple's New Privacy Labels.* https://www.nytimes.com/2021/01/27/technology/personaltech/apple-privacy-labels.html

[27] Alice Torjussen and Holly Root-Gutteridge. 2020. Is Nothing Better Than Something? A Preliminary Investigation into Disembodied Stimuli for Home Alone Dogs. In *Proceedings of the Seventh International Conference on Animal-Computer Interaction*. 1–6.

[28] Heli Väätäjä, Päivi Majaranta, Poika Isokoski, Yulia Gizatdinova, Miiamaaria V Kujala, Sanni Somppi, Antti Vehkaoja, Outi Vainio, Oskar Juhlin, Mikko Ruohonen, et al. 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*. 1–12.

[29] Heli Väätäjä, Päivi Majaranta, Heini Törnqvist, Mari Ainasoja, Veikko Surakka, Oskar Juhlin, and Clara Mancini. 2017. Technology for Bonding in Human-Animal Interaction. In *Proceedings of the Fourth International Conference on Animal-Computer Interaction*. 1–5.

[30] Junia Valente and Alvaro A Cardenas. 2017. Security & privacy in smart toys. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. 19–24.

[31] Dirk van der Linden. 2021. Interspecies information systems. *Requirements Engineering* (2021), 1–22.

[32] Dirk van der Linden, Brittany I Davidson, and Anna Zamansky. 2019. The not so secret life of pets: pet owners' privacy concerns for pet location data. In *Proceedings of the Sixth International Conference on Animal-Computer Interaction*. 1–6.

[33] Dirk van der Linden, Emma Williams, Irit Hadar, and Anna Zamansky. 2019. Some might freak out: What if your dog's activity tracker were to have a data breach?. In *Proceedings of the Sixth International Conference on Animal-Computer Interaction*. 1–12.

[34] Dirk van der Linden, Anna Zamansky, Irit Hadar, Barnaby Craggs, and Awais Rashid. 2019. Buddy's Wearable Is Not Your Buddy: Privacy Implications of Pet Wearables. *IEEE Security & Privacy* 17, 3 (2019), 28–39.

[35] Aviva Vincent, Hanna Mamzer, Zenithson Ng, and Kathleen J Farkas. 2020. People and their pets in the times of the COVID-19 pandemic. *Society Register* 4, 3 (2020), 111–128.

[36] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

[37] Anna Zamansky, Dirk van der Linden, Irit Hadar, and Stephane Bleuer-Elsner. 2019. Log my dog: perceived impact of dog activity tracking. *Computer* 52, 9 (2019), 35–43.

APPENDIX

A QUESTIONNAIRE

(1) What breed is/are your dog(s)? [open question]

(2) How old is/are your dog(s)? [open question]

(3) How much time do you typically spend with your dog(s) each day?
- Less than an hour
- A couple of hours
- Most of the day
- All of the day
- Other: [ ]

(4) Do you currently own any digital technologies for dogs?
- Activity tracker (e.g., FitBark, PitPat)
- Health monitor (e.g., PetPace)
- Smart toy (e.g., iFetch Frenzy Automatic ball launcher, Kong Wobbler)
- I do not own any digital technology for dogs
- Smart feeder (e.g., PetSafe Smart Feed)
- Pet cameras (e.g. Furbo Dog, Tapo)
- Other: [ ]

(5) If you own any digital technologies for dogs, what do you like most and least about them? [max 100 words]

(6) If you do not own any digital technologies for dogs, what would be the main factors for you in deciding whether to purchase them? [max 100 words]

(7) What data do you think digital technologies for dogs typically capture of you and your dog?

(8) Do you typically read privacy policies when you buy a new device for yourself? [yes/no]

(9) What would you find most important to see in the privacy policy of a technology for dogs? Please be as detailed as possible. There are no wrong answers, we are interested in all your thoughts! [max 300 words]

(10) Here are some statements about privacy policies in general. To what extent do you agree with the below statements? [5pt Likert, anchored with "strongly disagree" and "strongly agree"]
- Privacy policies use too much legal language
- Privacy policies take too much time to read
- Privacy policies are too complex to read
- I would prefer shorter privacy policies

(11) What gender do you identify with?

(12) What is your age?

(13) What country do you live in