frontiers | Frontiers in The Internet of Things

TYPE Original Research
PUBLISHED 07 December 2023
DOI 10.3389/friot.2023.1281464

OPEN ACCESS

EDITED BY
Oktay Cetinkaya,
University of Oxford, United Kingdom

REVIEWED BY
Mehran Mozaffari Kermani,
University of South Florida, United States
Chanapha Bast,
Udon Thani Rajabhat University, Thailand
Shitharth S,
Kebri Dehar University, Ethiopia
Khalid Yahya,
Gelisim University, Türkiye

*CORRESPONDENCE
Scott Harper,
s.harper@newcastle.ac.uk

RECEIVED 22 August 2023
ACCEPTED 16 November 2023
PUBLISHED 07 December 2023

CITATION
Harper S, Mehrnezhad M and Leach M (2023), Security and privacy of pet technologies: actual risks vs user perception.
Front. Internet. Things 2:1281464.
doi: 10.3389/friot.2023.1281464

Security and privacy of pet technologies: actual risks vs user perception

Scott Harper[1]*, Maryam Mehrnezhad[2] and Matthew Leach[3]

[1]School of Computing, Newcastle University, Newcastle upon Tyne, United Kingdom, [2]Department of Information Security, Royal Holloway, University of London, Egham, United Kingdom, [3]Comparative Biology Centre, Newcastle University, Newcastle Upon Tyne, United Kingdom

As IoT becomes more and more commonplace, it is expanding into many different industries. One of these rapidly growing industries is pet tech, technologies designed to aid with the care of pets, expected to reach a market value of $3.7 billion by 2026. As with all IoT technologies, these devices introduce new security, privacy, and safety risks to their users and their homes. Despite these risks, the security and privacy (SP) of these devices, and their users' concerns regarding these issues, remain an under-researched field, leaving the users of these devices at risk of attack and unable to effectively protect themselves. In this paper, we perform two studies to address this research gap. First, we perform an SP analysis of 20 popular pet tech apps, finding serious security vulnerabilities, as well as poor SP practices. Among our findings, 2 out of 20 apps exposed user login and account details in non-encrypted traffic and 14 communicated with trackers before the user could consent. Second, we perform a user study of 593 participants across 3 different countries (United Kingdom, United States, Germany) to gain an understanding of what technologies are in use, incidents that have or they believe may occur, as well as the methods used by participants to protect their online SP compared to pet tech. We perform a demographic analysis of these results, finding many similarities across the countries and genders, as well as a few differences in concerns and expectations. We study the state of the security and privacy of pet technologies and the awareness, concerns, and desires of users. We find that 521 participants do believe that a range of attacks may occur targeting their pet tech. Despite this, they take fewer precautions with these devices, exposing themselves and their pets to the possible risks and harms of these technologies.

KEYWORDS

animal technologies, pet technologies, internet of things, user study, user security and privacy

1 Introduction

The presence of IoT devices within our homes is becoming more commonplace, growing faster than predicted, with 14.3 billion active IoT endpoints by the end of 2022, with an additional 16% growth expected by the end of the year (Vailshery, 2022; Sinha, 2023). Outside of human-focused devices, pet technologies, designed for use on or around pets are also becoming more common. The devices used are largely focused on cats and dogs and include wearable devices that can aid in tracking the health/fitness of the pet. GPS devices are also popular and can help prevent an owner from losing their pet. Other devices include smart feeders and water fountains, to care for the pet when away, as well as cameras to check

in on your cat or dog. Examples of these technologies can be seen in Figure 2. These devices can help provide peace of mind for owners, as well as easing their caregiving responsibilities, and promise to improve the quality of life for their animals.

Pet theft in the United Kingdom is a growing issue, seeing a year-on-year increase (Gather Cover, 2022). It will have an even greater impact on people with disabilities who may rely on an animal to aid them. A study of pet owners found 75% of them take additional security precautions to protect their pets (Gather Cover, 2022). If their solution is pet tech devices, then they will be introducing additional IoT devices within their home environment.

Despite these technologies being adopted by more pet owners, these devices are lacking in how they protect their users' security and privacy (SP). Yet this remains an underresearched area, with few pieces of work analysing the security and privacy of pet technologies. What research has been done casts a negative light on these technologies, showing security vulnerabilities and poor privacy practices.

As the demand for pet technologies increases (Research and Markets, 2019), the industry will continue to offer more solutions that are potentially not secure and expose the user to the risk of attack. These devices will collect data on and interact with multiple users within a household, possibly including children. Many of these devices feature a range of sensors, including cameras and microphones, as such, they may be used to exploit a user's security and privacy at many levels.

Although these devices may help protect against theft, attacks against these technologies may aid in these thefts through spoofing or the denial of access (Kohnfelder and Garg, 1999) to the GPS location information these devices may rely on. Attackers could also target the feeding devices used for pets (Baker and Green, 2021), which can also be used to dispense vital medication at set times. These attacks could be used to endanger the animal, enabling the attacker to demand a ransom from the owner.

Attacking these systems may also reveal some of the potentially personal data that is collected by these devices. This data can include the owner's location, address, and when they are home. Access to this data could enable further more serious attacks against the user, e.g., theft or access to further sensitive information.

Despite these potential risks, there is little research into the SP risks of these technologies (Van Der Linden et al., 2019a; Baker and Green, 2021; Harper et al., 2022a), as well as the users' knowledge and concerns with these devices (Van der Linden et al., 2019b). This paper contributes to the body of knowledge via two separate studies; an SP analysis of animal-based apps and a user study of pet tech users. Our studies aim to gain an understanding of both the technical and user aspects of these technologies, to identify current and future risks, as well as ways in which they may be avoided. More specifically, our research questions (RQ) include: RQ1: *What are the security and privacy practices of popular pet-based apps?* RQ2: *What are the concerns and practices of those using pet technologies?* RQ3: *How do user perceptions and concerns compare to the real risks?*

To answer the above, we conduct two different studies. In Study 1, we evaluate the SP features and practices of popular Android pet apps. We curated a dataset consisting of 20 popular Android apps designed for pets. This list has been made accessible to other researchers, enabling them to carry out additional studies. Additionally, we employed various SP evaluation techniques and tools; including static, dynamic, and network traffic analysis, as well as assessments of privacy notices and tracking in accordance with data protection regulations. This study identified serious security vulnerabilities, along with poor privacy practices across the board, with 2 out of 20 apps exposing user login and account details in non-encrypted traffic and 14 communicating with trackers before the user could consent. These security vulnerabilities were communicated with the companies responsible, upon retesting one of the apps is no longer putting the user at risk.

Study 2 focuses on understanding the awareness and concerns of those using these technologies. We achieve this by performing a user study of 593 pet owners from different countries. We design and distribute a survey to determine the technologies in use, why they are used, the advantages and disadvantages of these devices, the data collected and any incidents that have occurred or they believe may happen. Additionally, we asked about the precautions they take with their pet tech, as well as their general online systems, asking for any security features they would like to see included. Our findings reveal that 521 participants are concerned that attacks against them may occur, but do not utilise the same level of security measures compared to their general online security. Demographic comparisons are also made, finding similar discrepancies in terms of concern and actions.

Through these two studies, we highlight the vulnerabilities present in currently available systems designed around pets and the more lax approach the users of these technologies take regarding their security when using pet tech devices, despite many believing an incident may occur. Our results are important since they highlight the need for better regulations and enforcement in an area which is understudied, not regulated, and attracts less public attention.

Contributions: To the best of our knowledge, this is one of the very few (if not the only one) studies that look at pet app security and privacy (study 1) and user perception (study 2) at the same time. Our specific contributions are.

1. We analyse the SP of 20 popular pet apps using a range of tools and methods, and identify serious security and privacy issues. Additionally, we review the related legislation on animal technologies and data.
2. We disclose these issues to the companies and work with them towards fixing these vulnerabilities in the new versions of their apps.
3. We conduct a user study on pet owners, gaining an understanding of their SP concerns and practices regarding pet technologies, providing a quantitative and thematic analysis of our results.
4. We identify differences between the actual risks of pet technologies and user perceptions, suggesting recommendations for different stakeholders.

We review the use and growth of pet technologies, along with the relevant works in Section 2. This paper consists of two studies, we first present our legislation review and app study in Section 3. Our user study is then presented in Section 4. Section 3 and Section 4 each contain their corresponding methodologies, ethics, limitations, and results. We discuss the results of these two studies, as well as future work in Section 5,

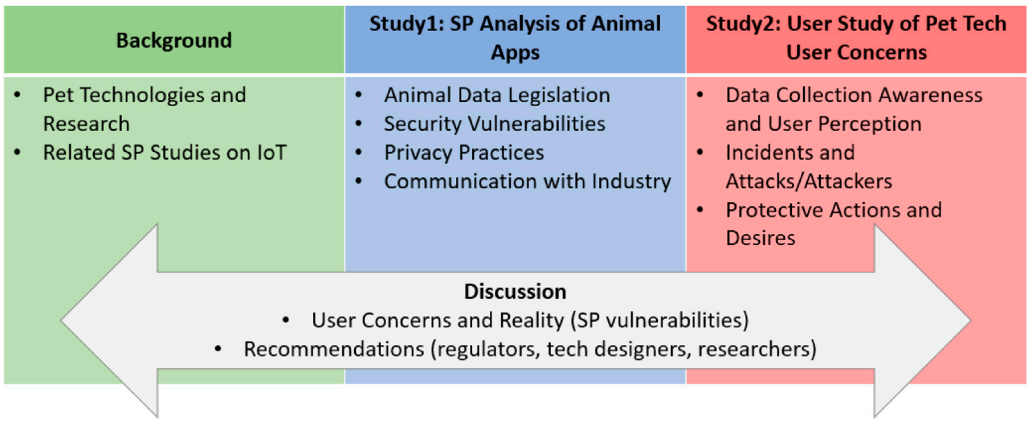

FIGURE 1
Overall scope of the paper.

concluding our paper in Section 6. The structure of our work can be seen in Figure 1.

2 Background and related work

In this section, we give background on these animal technologies, similar studies on smart devices, and the SP implications of these animal technologies.

2.1 Pet technologies

Smart devices for animals are becoming increasingly popular with veterinary wearables expected to reach a market value of $3.7 billion by 2026 (Research and Markets, 2019) and pet wearables had a market size valued at $1.6 billion in 2019 (Grand view Research, 2020). FEDIAF, the European pet food industry, reported the annual sale of pet accessories in 2020 as being worth $9.2 billion (Fediaf, 2021). Given the 2.8% annual growth of the pet food industry in 2020 (Fediaf, 2021) and the recent increase in pets in countries such as the United Kingdom (11% of households acquired a new pet) (PFMA, 2021), these sales are likely to grow as more people own pets and begin to adopt these technologies.

Pet wearables, such as activity monitors, are used for tracking a pet's exercise, activities, and fitness. GPS tracking devices give the exact location of an animal at a given time. These are typically used to help find lost pets and can include a "geofencing" feature that alerts you when your pet leaves a set area. Automatic feeders dispense food at set times every day, and may also be used to dispense the pet's medication. Cameras can allow the owner to keep an eye on their pet when they are away from home. Many devices also integrate cameras, e.g., feeders, treat dispensers, and water fountains (Catit, 2023).

There are also animal health applications that aid in tracking the pet's health, whilst providing information to help look after the pet. Examples of the systems mentioned by our participants can be seen in Figure 2. A diagram of the pet technology ecosystem can also be seen in Figure 3. This emphasizes the diverse user base of these systems and the interactions between users and animals within them. Here, numerous individuals may have access to a user's device or the data it captures.

Concerningly, these pet tracking devices may also be used to track things other than pets. One app, Tracki, advertises the use of its devices on people and objects as well, being named "Tracki GPS for child pet car" and has more than 20k users (Tracki, 2022). Van der Linden et al. found that people use pet trackers on children, the elderly and the impaired, with users unaware of the potential privacy implications of misusing these technologies that may not be designed with the same SP standards as those designed for humans (Van der Linden et al., 2020).

2.2 Security and privacy of apps

There have been a variety of previous studies looking into the SP of varying app groups. Focusing on the privacy aspect, Vallina-Rodriguez et al. use the Lumen privacy monitor tool to present insights into the mobile advertising and tracking ecosystem (Vallina-Rodriguez et al., 2016). This study of 690 users and 1732 apps, found that 60% of these connected to at least one domain (Vallina-Rodriguez et al., 2016). Following this, Razaghpanah et al., used the Lumen Privacy Monitor tool with 11,000 users and 14,599 apps, identifying 2,121 trackers (Razaghpanah et al., 2018). In a study of the top 116 EU websites and their corresponding apps, Mehrnezhad finds inconsistencies in how privacy consent banners are displayed to the user across platforms and find that the majority of these applications begin to track the user before the users can interact (Mehrnezhad, 2020). Focusing on the 30 most popular Android apps for women's fertility management, Mehrnezhad et al., find that the privacy of the user is not respected in these applications, and find no direct mention of fertility data in the GDPR (Mehrnezhad and Almeida, 2021).

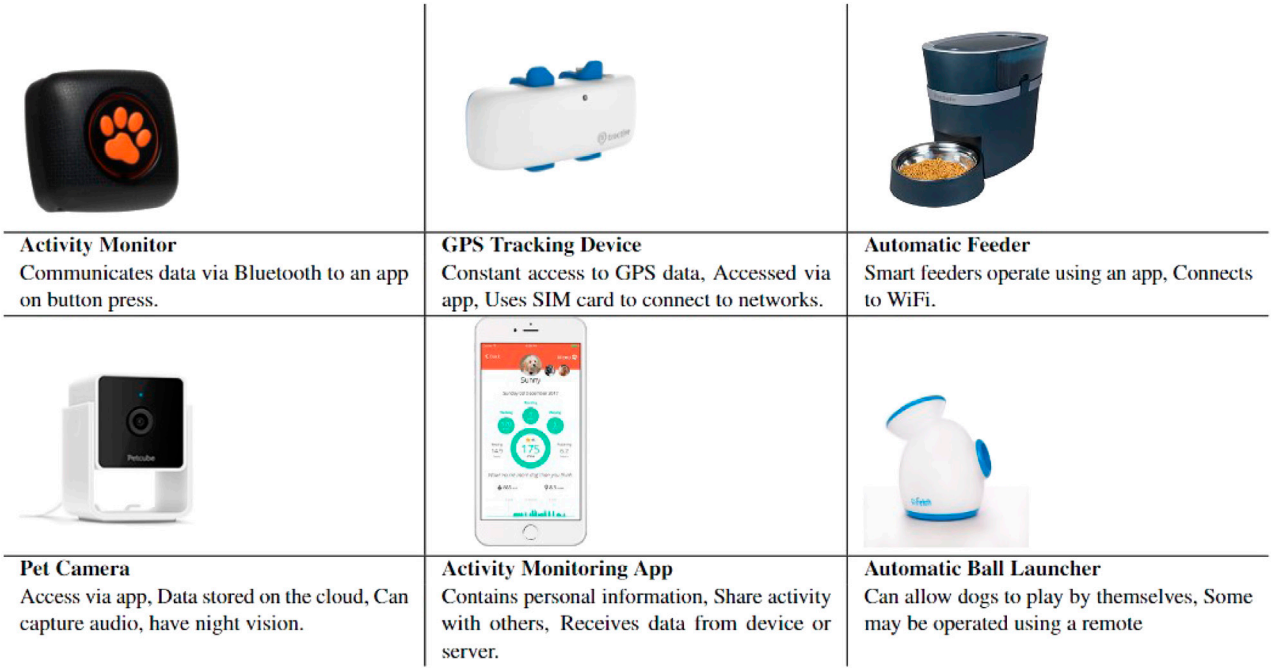

FIGURE 2
Examples of pet technologies used by the participants of the user study.

FIGURE 3
The pet technology ecosystem; showing how users interact with these systems. Other users may include vets, insurance companies, health clinics, *etc.* Arrows represent the flow of data.

A study by Mutchler et al. on mobile web apps (all available free web apps as of June 2014), found that 28% of the apps studied had at least one security vulnerability (Mutchler et al., 2015). A study by Aliasgari et al. focused on the top 25 health applications, analysing them for SP vulnerabilities. They examined the apps' use of TLS, finding that 12 of the apps revealed passwords when attacked (Aliasgari et al., 2018). A review and recommendations of mobile health app SP was performed by Martínez-Pérez et al. (2015). They provide suggestions around access control, authentication, data transfer and retention, as well as informing the patients before collection and after a breach. An overview of these papers can be seen in Table 1.

TABLE 1 Overview of previous SP app studies. * - also studied the corresponding websites. PI stands for Privacy International's data interception environment.

Paper	No. Apps	App type	Tools	Trackers	Traffic Analysis	Legislation Review	User study	Privacy notice Assessment
Vallina-Rodariguez et al. (2016)	1732	General	Lumen	✓				
Razaghpanah et al. (2018)	14,599	General	Lumen	✓				
Mehrnezhad (2020)	116*	General	Brave, Lumen	✓				✓
Mehrnezhad and Almeida (2021a)	30	FemTech	Lumen, Exodus	✓		✓		✓
Mutchler et al. (2015)	998,286	Web apps	apktool, Soot		✓			
Aliasgari et al. (2018)	25	Health	Wireshark, SSL Labs, Fiddler		✓	✓		
This Paper	20	Pet apps	Exodus, Lumen PI, Prolific	✓	✓	✓	✓	✓

2.3 User security and privacy concerns

One previous study has looked into the SP concerns of dog owners. In this study, the authors ask 61 users of this device about a hypothetical data breach (Van der Linden et al., 2019a). They find a lack of concern amongst these users, especially regarding the privacy of the data collected via these devices. With this lack of privacy concern and awareness of the risks, the authors argue that owners should be better informed about the privacy implications of the activity data captured. In Van der Linden et al. (2020), focused on privacy risks and concerns, Van der Linden et al. perform a study looking at product reviews for pet technologies. They find a lack of privacy concerns and discover that these devices are being used in different ways than intended, such as to track children.

Due to the lack of further user studies on the SP of pet technologies, we overview the concerns that users have about the use of smart technologies in their home environment. Many pet tech devices are being used in home environments and can be managed by similar smart home apps. Given the increased use of smart devices within home environments, there is likely an increase in SP risks. This is due to the introduction of more "vulnerable and unreliable devices" (Zeng et al., 2017), that are interconnected within the smart home environment and may also be connected to the internet. Previous research has shown that a malicious attacker can extract PIN codes and text messages from recordings collected by a voice assistant within a smart home environment via a side channel attack Zarandy et al., 2020).

Other studies such as (Emami-Naeini et al., 2017; Zeng et al., 2017; Zheng et al., 2018; Abdi et al., 2019; Chhetri and Motti, 2019; Prasad et al., 2019; Tabassum et al., 2019; Guhr et al., 2020; Harper et al., 2020; Taher et al., 2020; Harper et al., 2022b) have focused on the users' awareness and concerns regarding the SP of smart homes and buildings and the IoT devices within them. They find a lack of awareness of the potential risks caused by the use of these technologies, potentially due to incomplete threat models, but that the level of knowledge does not necessarily influence their threat models and concerns. They give suggestions to help alleviate concerns, e.g., better notification of users, more user-friendly settings, and taking the individual's preferences into account.

2.4 Security and privacy of pet technologies

Studying wearable devices, Van der Linden et al. find that these pet technologies, and their corresponding applications, actually capture more data about the owner than the pet (Van Der Linden et al., 2019b). This study highlights that these technologies should be designed around the SP needs of human users. A once commercially available dog activity tracker was shown to be vulnerable to a side channel attack by Levina et al. (2021). Through the use of an electromagnetic attack, they were able to capture and analyse the Base64 encoding algorithm by recording traces from the device's CPU. Mozilla's "*Privacy Not Included" (Mozilla, 2018) project provides consumers with an SP guide for smart products. Including several smart pet technologies, e.g., activity monitors, GPS trackers, cameras, and automatic feeders. To contribute to this research area, we perform two studies, an SP analysis of popular pet applications and a large-scale user study, looking at the SP concerns of pet tech users and compare our findings.

3 Study 1: Security and privacy analysis of animal apps

3.1 Review of legislation

In this section, we explain our methods for analysing a selection of legislation focusing on privacy and animal welfare and discuss our findings. Our aim here is to try and find mentions of these technologies, or SP, in animal-based legislation.

3.1.1 Approach

We selected the top-ranking animal welfare legislation, as ranked by World Animal Protection (2021) and Global Animal Law Association (2021), for our analysis. The animal welfare legislation that we look at includes those from Austria (Government of Austria, 2004), Denmark (Danish Veterinary and Food Administration, 2017), Germany (Federal Republic of Germany, 2006), the Netherlands (Government of the Netherlands, 2011), Sweden-(Swedish Ministry of Trade and Industry RSL, 2018), Switzerland (Federal Assembly of

Switzerland, 2005), England and Wales (Government of the United Kingdom, 2006), and (The World Organisation for Animal Health (OIE), 2021). We also look at the General Data Protection Regulation (GDPR) (EU, 2018) and California Consumer Privacy Act (CCPA) (State of California Department of Justice, 2018), along with its recent amendments (State of California Department of Justice, 2020) since they are the world-leading privacy legislation.

For the analysis of the animal welfare legislation, we first searched for a selection of keywords looking for mentions of these technologies. These included but were not limited to data, technology, sensor, privacy, security, wearable, personal, and sensitive. We additionally went through each of the sections to ensure that no security, privacy, or technology-related content had been missed. For the GDPR and CCPA, a similar process was used with animal-focused words (e.g., pet and wearable) and a review was done of the sections like before. We also discussed this area with experts in animal tech in academia and industry, confirming a lack of dedicated SP policies in these industries with SP not being considered by those designing and using these technologies.

3.1.2 Findings

There are currently no regulations for the collection and storage of animal-based data as the GDPR does not apply to data from which you can identify an animal (RCVS, 2018). Furthermore, there is no mention of animal applications, smart technologies, or the data that they collect in the current animal legislation in the (Government of the United Kingdom, 2006, Government of the United Kingdom, 2007), or the codes of practice for pet owners (Department for Environment, Food and Rural Affairs, 2017b; Department for Environment, Food and Rural Affairs, 2017a) despite the growing use of these technologies. The CCPA also has no mention of these animal-related technologies, focusing solely on the privacy of human data within systems.

A further review of the top-ranking animal welfare legislation finds little detail on these technologies. The closest being that new technologies can be tested on animals (Swedish Ministry of Trade and Industry RSL, 2018), the mention of radio frequency identification (RFID) in ear tags, and that electronic devices used in facilities should be safe for cattle (The World Organisation for Animal Health (OIE), 2021). In terms of animal data, the Swiss legislation states that it includes the data from monitoring animals and "the results thereof" (Federal Assembly of Switzerland, 2005). In Austria, pet-related data is removed after a fixed period, 20 and 25 years for dogs and cats respectively (Government of Austria, 2004), however, this is not for privacy reasons. The OIE mention the recording of production data for an animal health management system (The World Organisation for Animal Health (OIE), 2021), however, this is vague and there is no mention of online or smart systems.

Given the lack of regulation, animal applications that do not store any data relating to people do not need to follow the same restrictions as apps designed for humans. However, many of these apps do capture data about people or data relating to the actions of individuals. Considering this, many of these animal-based applications may not be designed to comply with the GDPR and other data privacy regulations such as the CCPA despite collecting data that may relate to individuals.

3.2 App review methodology

In this section, we explain how we prepared our app set, our SP evaluation methods and tools. We have conducted our experiments between Mar to July 2021 in the United Kingdom which is currently complying with the GDPR.

3.2.1 App set

A set of 20 pet-related applications were selected for analysis. Where possible, apps were selected from the device set used in Van Der Linden et al. (2019b). However, 9 of the applications for these devices were either not visible on the Google Play Store or were not fully functional. This resulted in 9 apps being used from this device set (1, 3, 4, 8, 10–12, 14, and 15 in Table 2). For the remaining apps, the most popular functional pet device applications were selected (2, 5–7, 9, 13, and 16 in Table 2). A selection of pet health apps was also selected to be analysed given the possibility that they may also capture data about their users. These 4 apps were chosen based on their popularity and the ability to create and log into an account (17–20 in Table 2).

3.2.2 GDPR requirements

To meet the GDPR's data protection principles, app and online service providers must make users aware of the tracking technologies involved in using their systems. Including informing the user what these tracking services do and why they are being used. They must get the user's consent to use this tracking data collected about them. The ICO (Information commissioner's Office, 2021) provides the following extensive guidelines on law-compliant practices. The service provider must present a way to gain consent from the user when they first access the application. The user must perform an unambiguous action, not linked to other matters such as terms and conditions. Providers must avoid the use of nudge behaviour and include accept and reject options. Consent is not valid if the user is blocked from accessing content without it. Highlighting the accept option is another form of nudging, which should be avoided. Users should be able to take back the consent that they have previously given as easily as they were able to give it. Providers should not rely on other outside mechanisms to determine the user's privacy control preferences, e.g., browser or mobile settings. Having the tracking technologies enabled before the user can explicitly give their consent via a positive action is a violation as consent has not been correctly obtained.

3.2.3 Methods

We use various methods to evaluate the SP of our set of apps (Table 2).

3.2.3.1 Static analysis

A method of analysing software that involves examining the code, but without executing it. This can be performed to identify certain names or features within a program's code. Android Lint[1] and SpotBugs[2] are

1 developer.android.com/studio/write/lint.

2 spotbugs.github.io.

TABLE 2 Table of Privacy Results - The analysed applications, their focus, number of users, and their corresponding privacy analysis results. Exodus and Lumen analysis results are shown under their respective columns. X in Lumen Column explained in Section 3.2.6. An explanation of Privacy Policy symbols can be seen in Figure 6.

No.	App	App	No.	Exodus	Lumen	Lumen	Privacy
	Name	Type	Users	Trackers, permissions	Trackers, permissions	Leaks	Policy
1	PitPat	Activity Monitor	10k+	4, 9	1, 13		✓
2	PoochPlay	Activity Monitor	1k+	5, 24	1, 24		X
3	CANINE	Activity Monitor	10k+	2, 13	X		-
4	PetPace	Activity Monitor	1k+	2, 10	1, 10		X
5	Weenect	GPS Tracker	100k+	3, 13	1, 13		X
6	PETFON	GPS Tracker	1k+	4, 25	1, 25	1	-
7	Trackimo	GPS Tracker	50k+	4, 16	1, 17		-
8	PawTrack	GPS Tracker	5k+	5, 14	0, 14		X
9	petTracer	GPS Tracker	10k+	0, 4	0, 5		X
10	Tractive	Tracker + Activity	500k+	7, 22	1, 18		-
11	Whistle	Tracker + Activity	100k+	5, 23	1, 15		X
12	FitBark	Tracker + Activity	10k+	5, 23	1, 24		-
13	Pawfit	Tracker + Activity	5k+	0, 26	1, 26	2	-
14	Kippy	Tracker + Activity	10k+	7, 18	0, 18		-
15	Scollar	Tracker + Activity	50+	2, 14	1, 15		X
16	Findster	Tracker + Activity	10k+	8, 35	3, 36		-
17	11pets	Pet Health	100k+	5, 17	0, 17		X
18	Joii	Pet Health	10k+	3, 19	1, 20		-
19	Dog Health	Pet Health	100k+	2, 10	X		-
20	DogLog	Pet Health	10k+	5, 10	1, 9		X

examples of static analysis tools that can be used to analyse programs for errors. Exodus Privacy[3] is the tool used in this paper and is explicitly designed for identifying trackers and what permissions are used for apps and has been previously used in (Mehrnezhad and Almeida, 2021).

3.2.3.2 Dynamic analysis

Involves testing or evaluating the program whilst it is running. Tools such as eclipse[4] can be used to test the performance of programs step by step while they are running. The tool Lumen Privacy Monitor[5] uses dynamic analysis for some of its features and was used in this paper due to its built-in focus on identifying trackers and permissions in Android applications. Lumen has shown to be an effective tool, being used in Vallina-Rodriguez et al. (2016); Razaghpanah et al. (2018); Mehrnezhad (2020); Mehrnezhad and Almeida (2021).

3.2.3.3 Network traffic analysis

Involves monitoring the network activity whilst using the program being analysed. This can help to identify anomalous network behaviour such as sending user information over non-secure traffic. It is typically achieved by intercepting the network traffic from the program, before passing it back on to its destination, like in an MITM. Android tcpdump captures packets from any "network connections you may have on your Android device"[6]. Whilst useful for capturing the packets, tcpdump does not allow the user to view encrypted traffic.

In this paper we used Privacy International's data interception environment[7]. This can decrypt the packets from HTTPS traffic, allowing them to obtain more information about the network activity of the selected applications. This tool has been specifically designed for the analysis of application privacy, making it ideal to use in this paper. It was previously used in

3 exodus-privacy.eu.org/en/

4 eclipse.org/ide/

5 haystack.mobi/

6 androidtcpdump.com/

7 privacyinternational.org/node/2732.

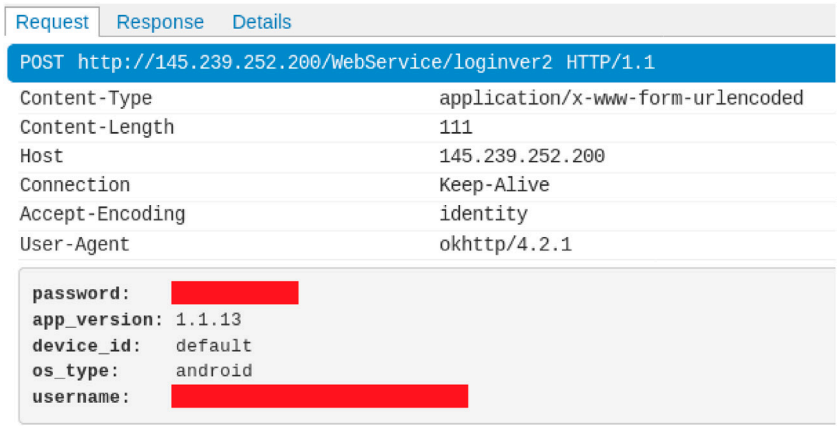

FIGURE 4
Example of a pet app revealing the user's login details. Login details have been anonymised.

Privacy International (2018), which highlights its effectiveness in monitoring an app's network activity.

3.2.3.4 Privacy notice analysis

To analyse the privacy policies of the selected applications they were opened on a prepared Android device. In each of the apps, we observe how the privacy policy is presented to the user. We look for whether the privacy policy is shown to the user upon first opening the app and, if not, whether it is displayed/mentioned during the account creation process available in the app. For apps where accounts cannot be created in the app, their websites were looked at via Google Chrome to see whether the privacy policy was clearly displayed to the user. This did not include the general privacy policies of some companies. Similar privacy policy studies have been conducted in Mehrnezhad (2020); Mehrnezhad and Almeida (2021). Note that some of the systems looked at required access to the physical devices they link to. If we could not create an account we looked at how the privacy policy was displayed on their website and if it was mentioned when requesting a demo.

3.2.4 Tools

Here, we explain the tools used in our experiments and their technical specifications.

3.2.4.1 Exodus privacy

Exodus Privacy is an online system that analyses Android applications, looking for embedded trackers by performing a "static analysis of APKs and compares the Java class names with a list of known trackers" (Exodus Privacy, 2020). Exodus produces reports listing the trackers and permissions, marking whether permissions are potentially dangerous. Exodus runs dexdump[8] on the application's extracted .apk file, giving all of the classes in the file. The list of known trackers is then checked against this list of identified classes (Exodus Privacy, 2018).

3.2.4.2 Lumen

Lumen is an Android app that uses dynamic analysis to identify trackers. Unlike Exodus, Lumen looks at the permissions requested by an app and the trackers communicated with whilst the app is being used. This can allow the user to view when an app is performing these communications/requests.

The selected applications were then run without further interaction, with Lumen active, and were left open for 2 h. This allowed us to capture the trackers communicated with before the user can interact with the app. The phone was left open throughout this time and used whilst the apps were running in the background. After the allotted time, Lumen was turned off and the apps closed. Analysis of the results involved counting through the identified trackers and permissions listed in the Lumen app. The results of this can be seen in Table 2.

3.2.4.3 Privacy international (PI)

This environment allows the user to capture all of the communications made through an Android phone. As well as this, PI is able to decrypt the captured data packets, allowing for the analysis of HTTPS traffic. Therefore this tool can be used to see whether user information, such as login information, is sent to any companies outside of those who run the app and whether it is sent securely.

When using PI, all applications were closed, ensuring only the selected app would be active. Mitmproxy[9] was then started, capturing all internet traffic going through the Android device. The selected app was then opened and, as a separate experiment, a login was completed where possible. Some applications were not able to be logged in to due to errors, such as Tractive, with other apps

8 android.googlesource.com/platform/art/+/master/dexdump/dexdump.cc.

9 mitmproxy.org/

FIGURE 5
User information displayed in plain text in the HTTP traffic of a Pet app. User details have been anonymised.

not allowing an account to be created due to a lack of the corresponding device. After being left for 10 min, mitmproxy was stopped and the results were analysed using mitmweb, allowing us to view the data being communicated, as seen in Figures 4, 5. Using this tool, we looked through the messages communicated to and from the app, looking for evidence of poor security practices when communicating the login details. These include the use of non-secure HTTP and a lack of encrypting the data prior to communication.

For both Lumen and PI, due to changes in how Android handles trusted credentials, a Google Pixel 3a was reverted to Android 9, allowing Lumen to install its own CA certificate. For PI, the device was also rooted, allowing for a CA certificate to be manually installed.

3.2.5 Ethics

Ethical approval was obtained through Newcastle University before any of the research took place. Due to the involvement of animal-based information, the project was approved by the Animal Welfare Ethical Review Body of Newcastle University too (ID 881). All our experiments were set up in a lab environment, i.e., there was no actual user and user data involved in our experiments. Working with the actual users of these products to measure their perception of risk and behaviour while working with these technologies is beyond the scope of this paper and is left as future work.

3.2.6 Limitations

An older version of Android had to be used to allow for both Lumen and PI to be used. This could potentially have affected the results if updates to the applications do not support past Android versions. Despite not being the most recent version, Android 9 and lower was used on 32.64% of United Kingdom Android devices in 2021 (Statista Research Department, 2022). Our experiments took place in March, April, and July 2021, where the percentage of users, in the United Kingdom, for Android 9 and lower was around 40% (Global Stats, 2021). Worldwide, it was more than 50% (Global Stats, 2022). This shows that a significant number of Android users would have been susceptible to an attack at the time of the experiments and a significant number of users would still be prone to the attack currently.

There is the possibility of Exodus giving false positives. Static analysis tools may detect trackers and permissions in the app's code that are never actually used. Even if not used, the presence of these trackers is still concerning as they may be used at a later point. We use our Lumen analysis to identify only the trackers communicated with during testing, before the user can consent. It may be the case that multiple other trackers become activated if a user engages with the app otherwise. Two of the apps (3 and 19 in Table 2) did not appear in Lumen. However, this likely just means that the app had not communicated with any trackers or requested any permissions within the time frame of our particular set-up in the experiments; shown through an X in the Lumen Trackers, Permissions column in Table 2.

Whilst running PI, several of the applications could not be fully opened or logged in to. This is possibly due to the applications making use of certificate pinning, meaning that they only trust specific certificates, which would prevent an attacker from decrypting the messages. This issue did prevent the testing of whether some of the applications communicate user information securely, however in the case of some of the apps, it may mean they are more secure against an MITM attack. Two of the applications (10 and 14 in Table 2) could not be opened whilst the environment was running. The apps would simply not load fully, with the environment reporting that they do not trust the mitmproxy certificate. Another three of the apps (3, 5, 15 in Table 2) could be opened, however, could not be logged in to whilst running the environment.

Some of the applications may have been able to hide their poor security practices from this analysis, being vulnerable to a more advanced attack. However, our analysis and findings are still vital as they highlight a clear and dangerous vulnerability that could put the users of these systems at risk. We specifically focused on the SP of pet solutions. We appreciate the complexity of the development and maintenance of these products, e.g., BLE pairing and communication encryption, e.g., lightweight cryptography in IoT environments (Turan et al., 2023). We consider these out of scope and leave it as future work.

3.3 Results

In this section, we discuss the results of the SP analysis as well as the results of our communications with the industry regarding the identified security flaws.

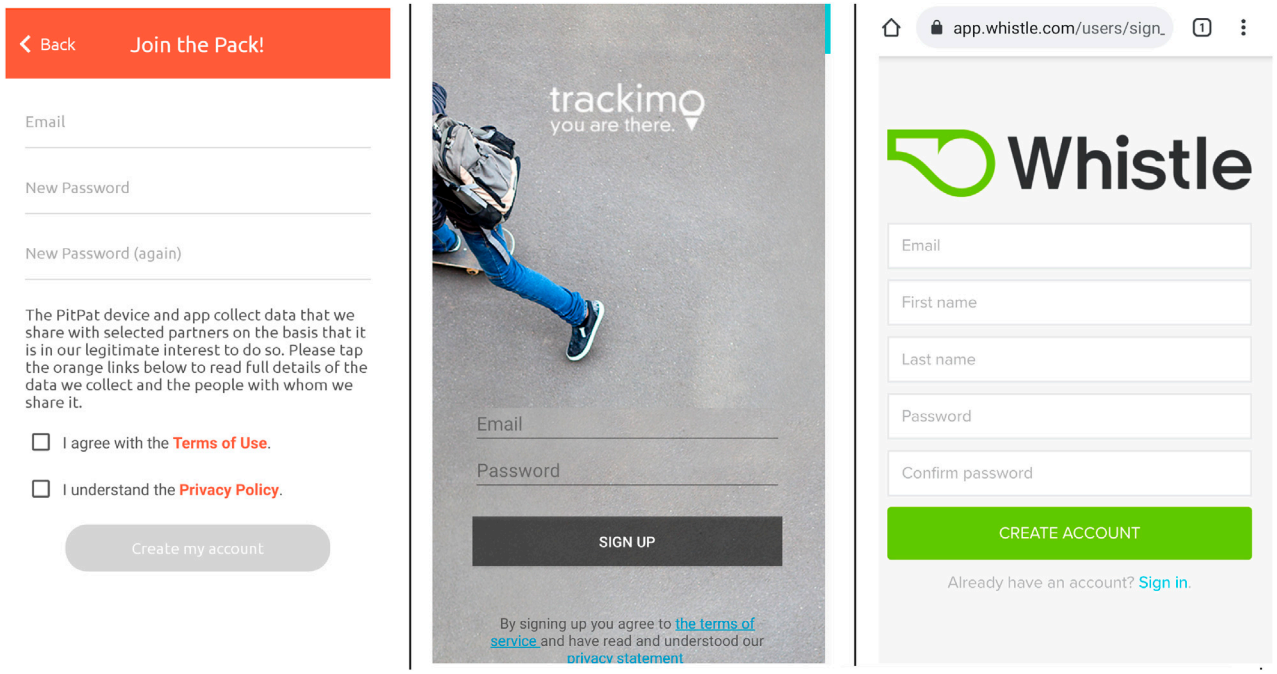

FIGURE 6
Account creation of 6 apps - Left (✓): PitPat; Middle (–): Trackimo; Right(**x**): Whistle ✓means that the privacy policy is clearly displayed to the user and that they explicitly have to accept it.–means that although the privacy policy is mentioned, it is either grouped with something else to be accepted or hidden through smaller text and positioning and just represented as a link. X means there is no mention of the privacy policy.

3.3.1 Security vulnerabilities

Serious security vulnerabilities were found in two of the applications, using the PI environment.

3.3.1.1 Password in plain text

Two of the applications studied (PoochPlay and Pawtrack) had the user's login details visible in plain text within non-secure HTTP traffic. This security vulnerability is incredibly concerning as anyone able to observe the internet traffic of someone using these apps will be able to find out their login information. An example of this can be seen in Figure 4. Collectively, these apps have over six thousand downloads, the users of which could be exposed to an attack due to this vulnerability.

The two applications, once accessed, will provide an attacker with information about the user and their pet. PawTrack's focus on GPS tracking will allow an attacker to see the exact location of the user's pet, an approximation of where the user lives, as well as the pet's past activity and paths. PoochPlay contains a variety of user information, such as their address and phone number, as well as the pet-related information that it collects.

3.3.1.2 User information in plain text

In addition to login information, these apps (PoochPlay and Pawtrack) also showed other user details that may enable an attack against a user. With PoochPlay, these details included the user's postcode and house number, as can be seen in Figure 5 (bottom). Details about the user's pet were also visible, including whether the pet can swim, medical conditions, medicines they take, and allergies. PawTrack exposes the user's latitude and longitude in plain text, giving the exact location of the user. This is alongside other user information such as their email, phone number, postcode, address, and the user's name; as seen in Figure 5 (Top).

3.3.2 Privacy vulnerabilities

As well as these security vulnerabilities, poor privacy practices were also identified.

3.3.2.1 Trackers

All but one of the applications was found to feature some form of tracking software. "A tracker is a piece of software whose task is to gather information on the person using the application, on how they use it, or on the smartphone being used" Exodus (2019). An increased number of trackers will mean that either more data is being captured about the user or it is being distributed to more third party services.

From the Exodus results, the GPS-related pet applications have a higher number of trackers (average of 4) and permissions on average than most of the other apps. However, pet Apps that have both GPS and activity monitor features have even more trackers and permissions on average (4.86).

In terms of the Lumen results, 14 of the apps were found to have at least one tracker. Apps that feature both GPS tracking and activity monitor features were again found to have the most trackers (average of 1.14). This was followed by activity monitoring apps (1), GPS trackers (0.75), and lastly pet health applications (0.67).

For permissions found by Lumen, tracking and activity monitoring apps again had the most (21.7 on average). This was followed by GPS trackers (17.25), activity monitors (15.67), and pet

TABLE 3 Design of the survey.

I) Demographics	II) Pets technologies	III) Risk-related questions
- User-related	- Usage	- Experienced incidents, - Predicted incidents, - Potential attackers
- Animal-related	- Advantages and disadvantages	- Protective actions (general, pet tech)
	- Data collection awareness	- Desired SP features, - Who is responsible for pet tech SP

health apps (15.33) respectively. Only two of the applications were found to have leaks from the Lumen analysis.

3.3.2.2 Privacy policy

Overall the apps perform very poorly in terms of notifying the user of their privacy policy, with only one of the apps getting you to explicitly agree to this, as seen in Figure 6. This app, 1 in Table 2, clearly displays the privacy policy to the user.

Ten of the remaining apps just provide a link to their privacy policy instead of displaying this to the user (the middle example of Figure 6). This goes against the requirements of the GDPR, which requires consent to be explicitly given by the users (Wolford, 2019), something that is unlikely to happen with most of these apps. Nine of the apps had no mention of their privacy policy when a user is registering an account or using the app, as can be seen on the right of Figure 6.

Another concern is that 14 of these apps are tracking the user in some way before the user has a chance to consent to this, as can be seen in the Lumen column of Table 2. As stated in Article 6 of the GDPR, the processing of user data can only be lawful if the data subject has given consent EU (2018). None of the apps allow the user to decline the privacy policy and continue to use the app. This goes against the GDPR as "you cannot require consent to data processing as a condition of using the service" (Wolford, 2019).

3.3.3 Communication with industry and Re-testing

After discovering these security vulnerabilities that may put the user at risk, the two companies behind the apps were contacted via email. This was to inform them of the vulnerability so that it may be fixed and to ask them how they would go about fixing the issue. They were contacted shortly after the final set of tests in July 2021. We wrote to these companies informing them about the enabling vulnerabilities and providing them with recommendations for fixing such flaws. We wrote to each company on at least three different occasions with 1 week between each email; making sure that such an email does not get ignored.

Out of the two applications with these security vulnerabilities, one of the companies replied to our emails to date. The company (PoochPlay) informed us that they had been planning on updating the app and would take our findings into account. As we received no reply from the other company, we are unsure if they are aware of this vulnerability and whether they have any plans to fix it.

We re-tested the applications with these serious security issues several months after communicating these issues to their respective providers. For this, we used the same methods as before, making sure that the applications were updated to their latest version. PoochPlay, the app that we heard back from, no longer reveals any user details. PoochPlay now operates more securely, using https for all of its communications. PawTrack, on the other hand, still presented the same issue as before. The user's email and password were clearly visible in an HTTP message. This lack of a fix is not surprising given that we did not hear back from its company.

4 Study 2: User study of pet tech users' concerns

Following on from our first study, we wanted to learn more about the SP awareness, concerns, and behaviours of those using these technologies. These findings would give insight into those using these devices, whether they are at risk and how they believe they can be better protected. For this, we distributed a questionnaire to a large number of pet owners.

In this section, we describe the process of designing and distributing our questionnaire. We give an outline of the participant's demographics and we discuss the methods used to analyse our results.

4.1 Methodology

4.1.1 Survey design

We start the survey by briefly introducing the relevant technologies to the participant. We then ask a short selection of demographic-based questions, the results of which can be seen in Table 4. We included the following for introducing pet technologies for the participants: "*Pet technologies refers to devices used on/for pets and includes wearable activity and location monitors, automatic feeders, microchips, and pet health apps, etc.,*"

The structure of the survey, including its questions can be seen in Table 3. We asked questions about the participants' demographics, their perception of pet tech and awareness of data collection, any incidents/attacks they are aware of or concerned about, and their protective actions and desired protective features. The specific questions are included on the top of the figures in the Results section. We use a mixture of open-text and multiple-choice for many of the questions to capture the participant's initial responses and then aid them with some suggestions if they are struggling to come up with a response. A combination of these responses is discussed, with any additional major themes being identified.

4.1.2 Analysis methods

For this paper, we have processed the collected data and represented the results through descriptive text as well as the use

TABLE 4 Participant Demographics. F: female, M: male, N: non-binary, one United Kingdom participant did not want to share their gender.

Country	Number	Mean age	Gender		
	Total: 593		#F	#M	#N
United Kingdom	199	36.19	118	76	4
USA	197	35.10	123	68	6
Germany	197	29.29	118	78	1

of bar charts and tables to help visualise our results. Where free text answers were given, we performed a thematic analysis taking an inductive approach where we allowed the data to determine our themes (Groß, 2017). Two of the authors performed coding and extracted the key themes. These themes were reviewed by both researchers and the results are reported, accordingly. The small size of our data allowed for accurate thematic analysis leading to uncovering visible patterns. Quantitative analysis was performed on the multiple choice responses, incorporating free text responses where applicable and avoiding participant overlap. Additional demographic analysis was performed on these collected results.

4.1.3 Survey distribution and participants

To distribute our survey, we used Prolific[10], a user study distribution platform. Prolific enables the filtering of possible participants, allowing us to specify participants with a cat or a dog, as well as their country of residence.

We distributed the survey to participants across three different countries (United Kingdom, United States, and Germany), receiving responses from 593 in total. We received 199 responses from the United Kingdom, 197 from the United States, and 197 from Germany. These countries were chosen as they had the most available participants through Prolific. Aside from country of residence, the only other factor taken into account when choosing the participants was whether they had a pet.

The mean age of the participants was 33.5, with the United Kingdom, United States, and German participants being on average 36, 35, and 29 respectively. For gender, roughly 61% of the participants were female, 37% male, and 2% non-binary, with one participant choosing "prefer not to say". All participants who fully completed the survey had a pet, with 511 (86.2%) stating that they use at least one form of pet-related technology. Further demographic information can be seen in Table 4.

4.1.4 Limitations

When screening, we could not specify that the participant uses pet technologies. Despite this, 511 of our 593 participants state that they do use some form of pet technology. Given the use of a study distribution service (Prolific) to obtain our results, there is the possibility of biases being introduced. These include rapid-responder bias, selection bias, maximum reward-per-hour bias (satisficing), and the WEIRD bias (Western, Educated, Industrialized, Rich and Democratic individuals) Prolific Team (2022). However, Prolific is aware of these biases and works towards minimising their impact on the research Prolific Team (2022). There is a slight presence of this WEIRD bias, with 60% of our participants being female, which is expected through Prolific. We are not aware of any further biases in our results.

4.1.5 Ethics

This research includes collecting data from users and had full approval from Newcastle University's Ethics Committee before the research commenced. In addition to having undergone independent ethical review, we designed our user studies to address pillars of responsible research in computer science (Menlo Report) (Bailey et al., 2012): respect for persons, beneficence, justice, and respect for law and public interest. Participation in this study was completely voluntary and anonymous. Collecting data through Prolific provided complete anonymity for participants with none of their personally identifiable information being revealed to us. All data collected can only linked back to their account number and not to the actual participant. Additionally, all participants provided informed consent, passed our screening question, and entered our completion code into Prolific, allowing us to confirm their participation. Participants were compensated a fair amount (average as recommended within the system).

4.2 Results

In this section, we discuss our results, highlighting the key findings from our analysis. All questions were required, meaning all responses are out of the total 593 participants.

4.2.1 Pet technologies

From our results, we have identified a variety of technologies being used on/for the participants' pets. The most common responses were microchips, GPS/location trackers, automatic feeders and cameras. Multiple participants mention using some form of mobile app, typically for health purposes, however, one participant mentions a *"dog community app"*. There are also multiple mentions of smart toys for pets, with one participant talking about an *"automatic ball launcher"*. Aside from cats and dogs, tortoises, chickens, and rabbits were mentioned by two participants each, with mentions of an *"Automatic door"* to ensure the safety of their animals. Donkeys and fish were each mentioned once by separate participants, with automatic feeders being used to aid in the care of the participant's fish.

10 prolific.co/

4.2.2 Data collection awareness

As seen in Figure 7 (where the results are split by the country of the participants), the name of the owner was the most selected option, followed by the address/location of the owner, basic pet info, contact info, microchip ID, pet location, and pet lifestyle, with these being selected 313, 296, 295, 291, 231, 227, and 210 times respectively. The remaining options were selected in the following order: pet image/sound (123), the age/gender of the owner (102), pet health (66), owner images/sound (49), payment information (37), pet technologies used (35), and other (35).

Pet lifestyle refers to the pet's activity as well as the information related to them being fed, e.g., timing, portion size and food type. Participants made comments such as *"The food habit of my dog and the amount of the single meals"* or *"weight, nutrition data, mood, mileage"*. Image/sound responses refer to possible pictures, videos, or audio recordings of the owner or pet, e.g., *"The camera can also record my movement when at home"*. Pet health includes *"Dog Weight, Heart BPM, calories, exercise level . . . "*, as well as *"medical information when they have last had treatment"*.

Additionally, the participants mentioned the collection of vet-related information (22) with participants mentioning *"vet registration number"* and *"His pet record"*. A small number of participants (13) also brought up the collection of social media-related information. There were also several mentions of these devices capturing the "typical" types/amounts of data, with one participant saying *"Probably everything that Apple already collects"*.

4.2.3 Advantages and disadvantages

4.2.3.1 Advantages

The most common benefits given were ease of use, improved pet welfare, convenience/saving time, and accuracy. These were selected or mentioned by 435, 414, 307, and 303 participants respectively. This was followed by increased knowledge about the owner's pet (250), finding the pet or preventing loss (215), these devices being secure (211), the peace of mind pet tech devices can provide (153), and the cost-effectiveness of these technologies (153). These results can be seen on the left side of Table 5.

Pet welfare here refers to *"prevent[ing] a pet getting lost"*, as well as *"hoping to prevent disease and li[v]e in good health"*. The convenience category largely captures the aspect of saving time through using these devices, e.g., *"using an app to book this is easier to fit into people's everyday life"*, and *"it keeps all the information together and at hand"*.

Some additional advantages mentioned by the participants include *"more control"* and *"Data may help science"*. Another participant mentioned a different type of practical advantage with *"dog stops barking when [the] device makes a sound"*.

4.2.3.2 Disadvantages

The main disadvantages identified were the costs involved with these devices, SP concerns, and possible inaccuracies or faults that may occur within these technologies, mentioned by 319, 187, and 102 participants respectively. The next most common disadvantages were the physical drawbacks and/or limitations of these devices (97), having a negative impact on the pet's safety (90), being a waste of time or too difficult to use (63), and the drawbacks relating to the continued maintenance of pet technologies (42), as seen on the right in Table 5.

"S&P concerns" includes security concerns around potentially being *"hacked"*, as well as concerns around data storage, e.g., *"Data about my pet and I being stored remotely"*. In terms of privacy, many participants showed concerns around *"Too much shared info"* and the *"Leak of data"*. Location data was specifically mentioned by some

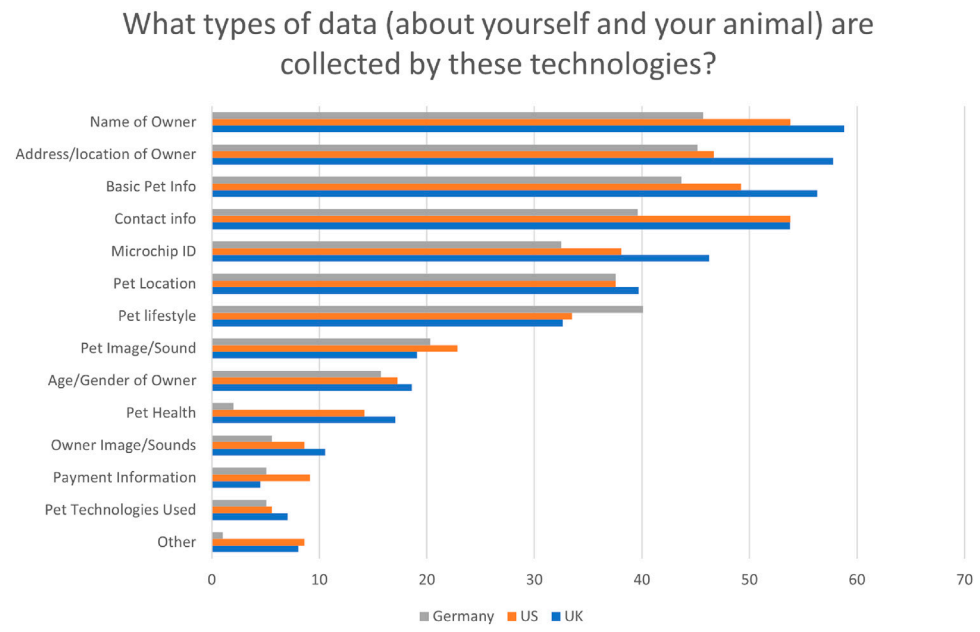

FIGURE 7
Percentage of participants from each country who believe that pet tech devices gather the following data.

10.3389/friot.2023.1281464

TABLE 5 Perceived advantages and disadvantages of pet technologies. Reported by users (593).

Advantages of pet tech		Disadvantages of pet tech	
Easy to use	435	Expensive	319
Improve pet welfare	414	SP concerns	187
Convenience	307	Possible inaccuracy/fault	102
Accurate	303	Physical drawbacks and limitations	97
Increase pet knowledge	250	Bad for pet safety	90
Find pet/Prevent loss	215	Waste time	63
Secure	211	Maintenance	42
Peace of mind	153		
Cost-effective	153		

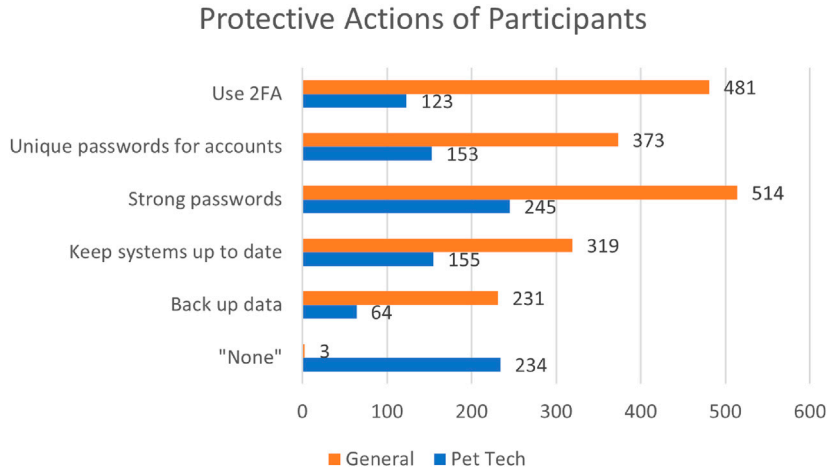

FIGURE 8
Protective actions reported by the participants for general SP vs. pet tech. *X*-axis is the number of participants.

of the participants showing concerns such as *"Other people could know where me and my dog is right now"*.

Other identified themes included concerns around these technologies removing owners from their pets' lives and care, with mentions that their *"[pets] might perceive it negatively"*. This was mentioned by 30 participants, along with *"Over reliance on unnecessary tech"*.

4.2.4 Incidents and attacks

4.2.4.1 Experiences of unpleasant incidents

For the incidents that have occurred, participants chose "Device stopped working" the most, with 132 selecting this option. "Unable to access account", "Data leak", "Harm to pet", and "Someone else accessing your account" were chosen 35, 9, 7 and 6 times respectively. No participants selected the option "Harm to human user" and we received 409 responses of "none" or equivalent.

Aside from the provided options, we also received 8 other responses. These refer to less significant inconveniences such as difficulty setting up, pets taking off devices, and pets chewing through cables. Some participants also mention a negative impact on the behaviour of their pets. One participant expressed concern as they have *"no control on chip data"*, with the company having complete control over it. Some more serious issues were also mentioned, with one participant mentioning the misuse of shock collars to harm pets, saying *"I think he enjoyed having that power over the dog"*. Another participant mentions their friend using a camera device that resulted in *"Burning down their house and killing the dog"*.

4.2.4.2 Predicted incidents

"Device stopped working" was, the most selected option, chosen by 330 participants. "Data leak", "Unable to access account", "Someone else accessing your account", "Harm to pet", and

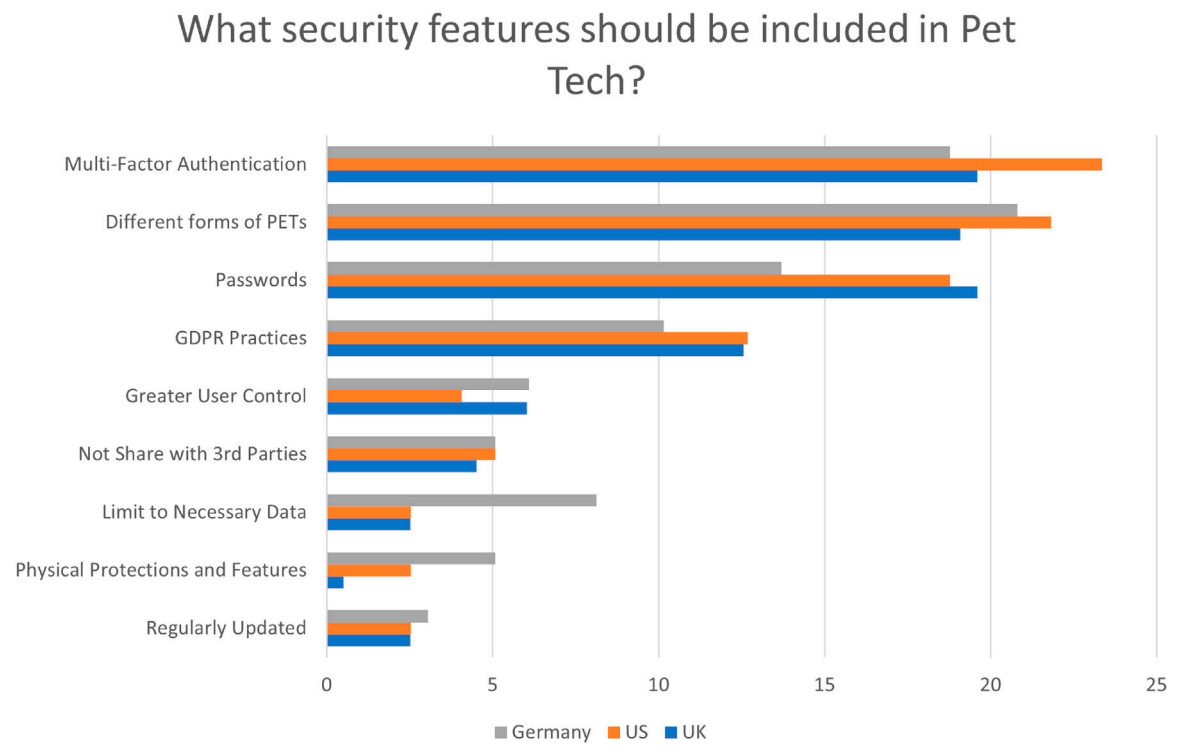

FIGURE 9
The desired protective measures of the participants for pet tech. *X*-axis is the percentage of participants from each country.

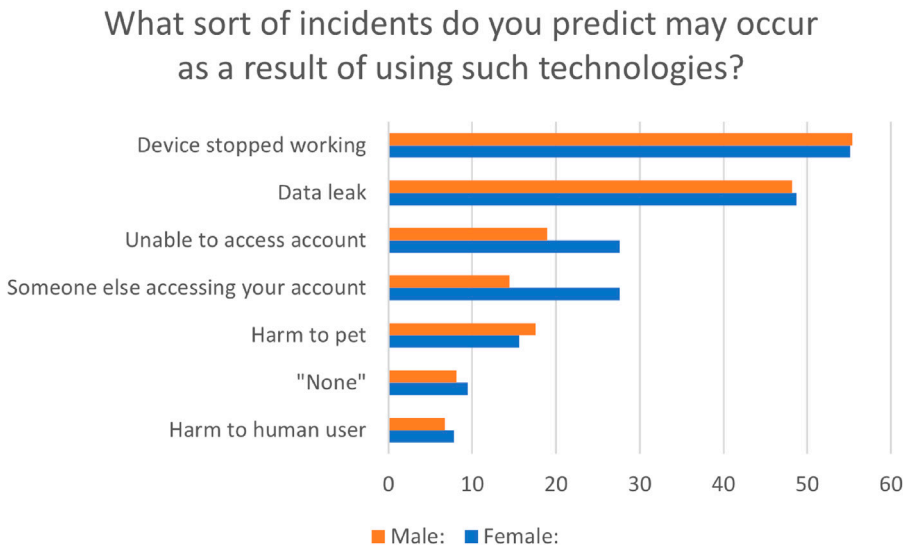

FIGURE 10
Gender comparison of the incidents participants believe may occur. *X*-axis is the percentage of participants in each gender. Given the far smaller number of responses by non-binary and "prefer not to say" participants, these groups have been excluded from percentage-focused figures, where their results may appear misleading.

finally "Harm to human user" were selected 287, 146, 136, 95, 44 times respectively, as can be seen in Figure 10. 72 participants responded with "none" or equivalent. There were additionally multiple concerns over devices no longer working correctly and *"becoming inaccurate"*, including *"over or underfeeding"*. As can be seen, there is a gap between the real-life experiences of the

participants and those that are of concern. While the participants' experiences are not significantly associated with security, privacy, and safety risks, the speculative concerns are. For instance, 287 participants (48%) believed that "Data leak" can be a risk to the users of these technologies.

4.2.5 Potential attackers

For possible attackers on these pet systems, participants selected the option "Cyber criminals" the most, selected by 327 participants. Followed by "Criminals", "third parties", "Insurance companies", and lastly "Activists", being selected 251, 233, 75, and 48 times respectively. The participants responded with "none" or equivalent 85 times.

Aside from the provided options, two participants mention the *"Government"* as a potential attacker. Several participants say that the attackers could be *"just people"*, who are potentially *"bored"* or *"have nothing better to do"*. One United States participant, brings up the possibility of an *"Estranged family"* member being an attacker, with this participant previously expressing concerns over the possibility of stalking *"by kidnapping their pet and scanning their chip"*. While some of these responses were brought up by a small number of our participants, they indicate potential research directions, e.g., in the context of intimate partner violence (Cleary et al., 2021; Giesbrecht, 2022).

4.2.6 Protective actions

4.2.6.1 General online security and privacy protection

For methods they use to protect their general online SP, "Strong passwords" was the most selected option, being chosen 514 times. Followed by "Use 2FA", "Avoid clicking unfamiliar links", "Avoid emails from unknown sources", "Unique passwords for accounts", "Keep systems up to date", "Back up data", and then "Use a password manager", which were selected 481, 455, 438, 373, 319, 231, and 186 times respectively, as can be seen in Figure 8. Only 3 of the participants responded with "none" or equivalent. An additional 3 options included "using a password manager", "avoid emails from unknown sources", and "avoid clicking unfamiliar links". These were chosen 186, 438, and 455 respectively. Apart from these options, 3 different participants mention the use of a VPN to ensure their online SP. 2 participants say that they use *"cyber security software"* of some kind to protect themselves. There is also the mention of using *"3 factor authentication"* by one participant.

4.2.6.2 Pet tech protective methods

For protecting the SP of their pet technologies, "Strong passwords" was again the most selected option, being selected 245 times. Following this, "Keep systems up to date", "Unique passwords for accounts", "Use 2FA", and finally "Back up data" were chosen 155, 153, 123, and 64 times respectively. The response "none", or equivalent, was given 234 times. Outside of these options, several of the participants mentioned less technical methods of ensuring safety, such as *"my pet stays indoors"* and *"keep away from water"*. On the more technical side, we had responses such as *"using data security device"*, *"my devices are not connected to WiFi"*, and *"Keep them separate from my other technologies and accounts"*.

4.2.6.3 Desired protective measures

For desired protective measures, variations on multi-factored authentication were by far the most common option, mentioned by 122 participants. Different forms of PETs (privacy enhancing technologies) such as strong security, encryption, biometrics, and vague mentions of stronger security were also mentioned by 122 participants. Passwords (103) and following GDPR practices (70) were the next most mentioned themes. The rest of the identified themes are; greater user control (32), Not sharing data with third parties (29), limiting the collected data to only what is necessary (26), mentions of physical protections and features focusing on the hardware side and preventing malfunction (16), and the regular updating of these technologies by those that design them (16).

The GDPR practices theme encapsulates ideas around following regulations, e.g., *"As long as they follow data protection protocol"*. It also covers security and transparency around the data, e.g., *"clear who has access to your data"*, *"alerts if someone attempts to use your email to login"*. Participants also mentioned *"guarantees"* of the SP of these systems. Greater user control covers a variety of controls focusing on security (physical and data) and privacy, including requests by the participants for protections on specific pieces of data, largely their location data. They also mentioned the ability to *"opt-out"* and *"A safety shut off"*.

4.2.7 Who is responsible for pet tech SP?

For who is responsible for taking care of the SP of these systems, the owners of the system and the companies that design them were by far the most selected options. These were chosen by 464 and 414 participants respectively. Following these, the other people that use these systems, the government, and third parties were selected 127, 64, and 38 times respectively. For additional responses, multiple participants expressed that they are unsure of who should be responsible. Some other answers include *"ISP"*, *"Companies hired for security"*, and *"Apple"*.

4.2.8 Participants' additional comments

Additional comments included General Positive comments about pet technologies (24), SP Worries/Concerns (15), Mentions of a lack of awareness and/or wanting to know more (11), comments about their Lack of Concern with these devices (6), and mentions of the Costs relating to these devices (4).

5 Discussion

In this section, we discuss our results, compare the findings of our studies as well as with the related work, and explore future directions for this research.

5.1 Security and privacy of pet apps

Our results show that 2 of the analysed applications (that are used by 6k + users, collectively) have a serious security vulnerability that reveals the user's login details. Another 8 applications were observed to handle user data poorly from the Privacy International analysis. Six of these applications (4, 7, 12, 16, 17, 18 in Table 2) had the user's login details visible in https messages and the remaining 2 had images visible, the first being the user-assigned pet picture, and

the second showing an image of the user's location (20 and 6 in Table 2 respectively). While secure against basic traffic interception and observation, it is bad practise and could put the user in danger if the attacker is capable of decrypting the messages as done in this paper.

In terms of privacy, we found that 18 (90%) of the popular pet apps studied have at least one tracker and that 9 (45%) have at least five (from Exodus results). Our studied apps are more likely to have a tracker than those studied in Vallina-Rodriguez et al. (2016) (60%) and Razaghpanah et al. (2018) (75%), analyses of more general apps using Lumen. As observed in Privacy International (2018), we also identified instances where apps established communication with trackers before obtaining user consent, finding this to be the case for 14 (70%), as seen in Table 2, compared to 61% of theirs communicating specifically with Facebook.

The apps also performed poorly regarding their privacy policy with only one app clearly displaying this to the user and requiring the user to explicitly agree to it. Similar poor privacy notice practices were found in Mehrnezhad (2020) and Mehrnezhad and Almeida (2021), studies of the top 116 EU websites and popular women's fertility Android apps. They found 51% and 40% of their apps respectively have no privacy notice, compared to 9 (45%) of our studied pet apps.

Overall, these results show that there are vulnerabilities and poor practices present within the popular pet apps available. If exploited by an attacker, these vulnerabilities could put the users of these pet technologies at risk. Additionally, the apps do not respect the user's privacy and do not effectively gain their consent before communicating with tracking services.

This part of our research received international media attention (Feb-March 2023) including an article in the Telegraph[11] on how pet-tracking apps may be "secretly snooping on owners", and an interview with the Naked Scientist[12], where we discussed the potential data collected, risks and vulnerabilities of these devices. This media attention shows interest from multiple stakeholders, including the public as the end users of these technologies, to understand the risks and harms associated with animal tech and improve their practices to protect their security and privacy. Informed by this, and other conversations that we had with experts in the field, we decided to dedicate the next part of our studies to the user dimensions of this topic by conducting our user study.

5.2 Security and privacy concerns of users

The study revealed that the participants utilized an array of pet technologies beyond microchips. A notable percentage of participants incorporated trackers, cameras, automatic feeders, and automatic water fountains into their pet care routines. Hence, the reported SP issues are in relation to the use of a wide range of pet technologies.

Although few participants encountered any negative incidents while using their pet technology, a considerable number expressed apprehensions about potential future occurrences. We identified concerns surrounding potential data leaks (exposing their personal information) and unauthorised access to their account, indicating their unease about potential attackers gaining access to their data. While a smaller number of participants believed that their pets or human users might be endangered, we still identified concerns regarding the safety of their pets. These findings indicate that the majority of users perceive their data as the primary target but also recognize the potential risk of harm to their pets.

For safeguarding their data, there were some similarities in the patterns of the responses for protective methods for general SP vs. pet technologies. In both cases, "Strong passwords" are the most popular method. However, there is a noticeable contrast in the level of precautions taken by participants concerning general online use and pet technologies, as depicted in Figure 8. Significantly fewer participants opt for precautionary measures with their pet technologies. This observation suggests that users tend to perceive the risks associated with pet tech devices and systems as less severe, and consequently, they may consider attacks against them to be less threatening. This perception persists, despite our findings indicating a belief among participants that various forms of attacks could indeed transpire when utilizing these technologies.

SP concerns were also mentioned in the disadvantages, with it being the second most selected option. However, this was still significantly less than the cost of the device, showing that the SP of these devices may not be the main focus. One potential explanation for this discrepancy is a lack of awareness regarding the potential risks associated with the data captured by these devices. Similar knowledge gaps have been observed in studies on other smart technologies similar to pet tech. Studies focusing on technologies and sensors utilized in smart homes and buildings have revealed users' limited awareness of potential risks (Emami-Naeini et al., 2017; Zeng et al., 2017; Zheng et al., 2018; Abdi et al., 2019; Chhetri and Motti, 2019; Prasad et al., 2019; Tabassum et al., 2019; Guhr et al., 2020; Harper et al., 2020; Taher et al., 2020; Harper et al., 2022b). However, in those cases, the lack of knowledge did not significantly impact users' levels of concern. This disparity may instead be attributed to the perception that the data collected by pet tech devices do not pertain to the users themselves but rather to their pets, which they may consider harmless. Research conducted by Van der Linden et al. in Van Der Linden et al. (2019a) has demonstrated that these assumptions are incorrect.

Our study yields comparable results to the findings of Van der Linden et al. (2019b), which examined concerns of dog activity monitor users regarding potential data breaches. Both studies underscore a lack of concern among users regarding the data collected about their animals. Similar to Van der Linden et al. (2019a), our results indicate that users are more concerned about the safety of their pets than themselves. This is shown by twice the number of responses predicting potential harm to the users' pets compared to harm to themselves. The most selected possible incident is that the pet's device will stop working. While harm to the user was not commonly mentioned by our participants, it is worth noting that other research explores such possibilities, particularly in the context of intimate partner violence (Cleary et al., 2021; Giesbrecht, 2022). Similar research in other

11 telegraph.co.uk/news/2023/02/28/how-dog-tracker-apps-snooping-humans-according-cyber-security/

12 thenakedscientists.com/articles/interviews/peoples-data-hacked-their-pet-apps.

emerging technologies, such as female-oriented technologies (FemTech), reveals that the data collected by connected devices are of interest to multiple threat actors, including former partners and family members, who may misuse it to harm the users (Mehrnezhad and Almeida, 2021; Almeida et al., 2022; Mehrnezhad et al., 2022b).

5.3 Demographic comparison

5.3.1 Country

German participants were slightly less likely to think that human/owner-related data is collected by these systems, as seen in Figure 7. There is not much difference between the countries for the advantages and disadvantages, but US and German participants focused more on ease of use and convenience. US participants were the most likely to discuss the aid these devices give for caring when away and providing peace of mind. For requested security features, German participants were slightly less likely to select features putting the burden on the system user and mentioned limiting to necessary data more than the other countries (Figure 9). They were also more likely to believe that third parties would be responsible for an incident and that the government should have some responsibility for the SP of these systems.

While we did not find significant differences between the countries and their understanding and concerns of pet technologies, previous research shows that such differences do exist. In Coopamootoo et al. (2022); Mehrnezhad et al. (2022a), the authors discuss how participants across three countries (United Kingdom, Germany, and France) show different patterns in their perception and feelings of online privacy and tracking and their protective actions. As future work, we plan to conduct a larger-scale study and research the differences and similarities across societies given the context of pet tech use, the available regulations, and other sociocultural elements.

5.3.2 Gender

Across the different questions, no significant differences were found between the responses of the male and female participants (adjusted for differing demographic group sizes). However, there were some differences identified concerning the different potential incidents that the participants believed may occur. As seen in Figure 10, female participants were more likely to show concern about someone else accessing their account and being unable to access their account. Despite these additional concerns about possible incidents with their devices, female participants were not more likely to take security precautions, both for their general online security and for their pet technologies.

Previous research shows that gender has an impact on user SP perception and practice, e.g., in Coopamootoo et al. (2022); Mehrnezhad et al. (2022a), the authors discuss how male and female participants demonstrate and express different feelings and mental models towards online privacy. Female users of these technologies do have additional risks that may account for these concerns, including the increased risks of intimate partner violence faced by women (Miller and McCaw, 2019). Multiple past incidents have involved ex-partners using a woman's pet as a means to get revenge (Gittens, 2014; Branagan, 2015). These possible risks/incidents may be further enabled or worsened by the presence of technologies that collect data about these female users. Our participants also mentioned concerns around stalking, with one participant saying *"if the technology could be hacked into, it could give others, for example, a stalker [an idea] of where a person may be"*. We would like to study the impact of gender more directly in the future via other methods such as Story Completion Method (SCM), where potential risky scenarios can be designed to be completed by participants. This method has become popular in SP research and sensitive contexts where the risks of tech abuse can be differentially harming based on gender, e.g., in intimate technologies such as female-oriented technologies (Mehrnezhad and Almeida, 2023; Moniz et al., 2023).

5.4 User concerns and reality

The participants of our user study did show concerns about possible attacks, especially female pet owners. However, we found little evidence of the participants experiencing a cyber incident relating to their pet tech devices. However, the results of our app study show that there are potential dangers in using these technologies, with very simple and easy-to-execute attacks being identified that may allow access to a pet owner's account. User details, such as their location and address were also leaked by these applications. Access to this information or their account may endanger users, enabling further real-world attacks against them.

Although we found vulnerabilities and the participants expressed that they believe an incident may occur, our user study shows pet owners taking fewer precautions when using pet technologies, potentially putting themselves at risk of attack. Given the differences between the precautions they take for pet technologies and general online tech, it is likely that those using these technologies take their security less seriously. The users of pet technologies are likely not aware of possible attacks or are not focused on this aspect when deciding to use them. Given these devices are largely used to aid with the health and safety of their animals, the cyber SP of the human owner is unlikely to be the priority. It is also possible that this disconnect demonstrates a lack of knowledge of how to effectively protect themselves when using pet tech or other IoT devices.

Notably, research in Van Der Linden et al. (2019b) reveals that many pet applications even gather more data about the human user than their pet, necessitating adherence to GDPR. Given such data is at stake, an attacker who gains access to the information captured by these devices could potentially track the human user, facilitating further crimes like robbery, burglary, or pet theft. Mere access to account details would aid in crafting phishing attacks targeting these users, enabling the impersonation of users in the social aspects of these apps. With the evident risks of potential attacks against their users, these apps must be designed with security measures to prevent the disclosure of user information to malicious parties.

5.5 Future work

Our work highlights a lack of awareness about the potential risks of introducing these internet-connected devices into these pet owners' lives. Further evaluation of the security of these devices and the proliferation of this information will help to keep the users of these devices informed and enable them to take the necessary precautions.

More general information about the risks of introducing IoT devices into people's homes and lives should also be made easily available, as many of the necessary precautions on the user's end can be applied more generally. As this market continues to grow, the SP complications will get more complex since these technologies are often shared in the household, e.g., with a partner and children. Work should be done to evaluate how these devices, and their connected systems, handle user data and whether they conform to the GDPR, communicating these results with the necessary groups where needed. Further user studies on this growing population of users should help to further inform the present risks, concerns, and desired SP features. Other potential research directions are performing and then mitigating attacks on IoT devices that are used for and on animals. This includes side channel attacks via the battery, motion sensors, and fault attacks. Stronger regulations on the security protocols used to communicate personal user details should be enforced to ensure all current and newly developed pet technologies do not put the user at risk. This sentiment was shared by many of our German participants, who felt the government should be more responsible for protecting users.

6 Conclusion

This paper provides an overall study of the pet tech environment, capturing both the security and privacy of these devices, as well as the views of those who use them. We perform both an SP analysis of 20 popular pet apps and an online survey of 593 pet owners from 3 different countries (United Kingdom, US, and Germany). Our findings highlight that not many users have experienced incidents with these devices, yet 521 of them speculate that there are a variety of potential incidents that may endanger either them or their pets. Our analysis of pet applications finds that security vulnerabilities are in fact present that could put them at risk, with 2 apps exposing user login and account details. Despite these worries and security issues, pet owners take far fewer precautions to protect the security of these devices, compared to what they do for their general online SP. We also find that the apps did not effectively respect the user's privacy with many of the applications violating the GDPR in some aspect, more specifically 14 communicated with trackers before the user could consent. We provide user-suggested features to improve the SP of these pet technologies. With this growth within the pet tech industry, the effects of these vulnerabilities will be further exacerbated if those designing and using these technologies do not take the necessary SP precautions. Given how sparse the SP research in animal tech is, we invite other researchers to further research the field in the hope of offering practical solutions to improve the quality of the lives of the animals and their owners without any risk and fear of the security, privacy, and safety of both the animals and owners.

Data availability statement

The raw data supporting the conclusion of this article will be made available by the authors, without undue reservation.

Ethics statement

The studies involving humans were approved by Newcastle University's Animal Welfare and Ethical Review Body (AWERB). The studies were conducted in accordance with the local legislation and institutional requirements. The participants provided their written informed consent to participate in this study.

Author contributions

SH: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Visualization, Writing–original draft, Writing–review and editing. MM: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Supervision, Writing–original draft, Writing–review and editing. ML: Conceptualization, Funding acquisition, Resources, Supervision, Writing–review and editing.

Funding

The author(s) declare financial support was received for the research, authorship, and/or publication of this article. This work was funded by the United Kingdom Engineering and Physical Sciences Research Council (EPSRC) through a DTP studentship (EP/T517914/1), and the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the United Kingdom EPSRC under grant number EP/S035362/1.

Acknowledgments

We would like to thank the management of Newcastle University Farms for their help in identifying animal technologies. We would also like to thank the participants of our user studies.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Abdi, N., Ramokapane, K. M., and Such, J. M. (2019). *More than smart speakers: security and privacy perceptions of smart home personal assistants*. SOUPS.

Aliasgari, M., Black, M., and Yadav, N. (2018). "Security vulnerabilities in mobile health applications," in 2018 IEEE Conference on Application, Information and Network Security (AINS) (IEEE), 21–26.

Almeida, T., Shipp, L., Mehrnezhad, M., and Toreini, E. (2022). "Bodies like yours: enquiring data privacy in femtech," in Adjunct Proceedings of the 2022 Nordic Human-Computer Interaction Conference, 1–5.

Bailey, M., Dittrich, D., Kenneally, E., and Maughan, D. (2012). The menlo report. *IEEE Secur. Priv.* 10, 71–75. doi:10.1109/msp.2012.52

Baker, L., and Green, R. (2021). Cyber security in UK agriculture. Available at: https://research.nccgroup.com/wp-content/uploads/2020/07/agriculture-whitepaper-final-online.pdf.

Branagan, M. (2015). Jilted boyfriend took revenge on ex by snapping their kittens' necks and mutilating their remains with a hammer. Available at: https://www.mirror.co.uk/news/uk-news/jilted-boyfriend-took-revenge-ex-5393743.

Catit (2023). Catit pixi vision smart dry food feeder with camera. Available at: https://catit.co.uk/products/catit-pixi-vision-smart-dry-food-feeder-with-camera.

Chhetri, C., and Motti, V. G. (2019). "Eliciting privacy concerns for smart home devices from a user centered perspective," in International Conference on Information (Springer), 91–101.

Cleary, M., Thapa, D. K., West, S., Westman, M., and Kornhaber, R. (2021). Animal abuse in the context of adult intimate partner violence: a systematic review. *Aggress. violent Behav.* 61, 101676. doi:10.1016/j.avb.2021.101676

Coopamootoo, K. P., Mehrnezhad, M., and Toreini, E. (2022). "I feel invaded, annoyed, anxious and i may protect myself": individuals' feelings about online tracking and their protective behaviour across gender and country," in 31st USENIX Security Symposium, 22. USENIX Security, 287–304. Available at: https://www.usenix.org/system/files/sec22-coopamootoo.pdf.

Danish Veterinary and Food Administration (2017). Danish animal welfare act. Available at: https://www.globalanimallaw.org/downloads/database/national/denmark/bekendtgorelse-af-dyrevaernsloven.pdf.

Department for Environment and Food and Rural Affairs (2017a). Code of practice for the welfare of cats. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/697941/pb13332-cop-cats-091204.pdf.

Department for Environment and Food and Rural Affairs (2017b). Code of practice for the welfare of dogs. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/697953/pb13333-cop-dogs-091204.pdf.

Emami-Naeini, P., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F., et al. (2017). *Privacy expectations and preferences in an iot world*. SOUPS.

EU (2018). General data protection regulation (gdpr). Available at: https://gdpr.eu/article-6-how-to-process-personal-data-legally/.

Exodus (2019). Trackers. Available at: https://reports.exodus-privacy.eu.org/en/info/trackers/.

Exodus Privacy (2018). Exodus static analysis. Available at: https://exodus-privacy.eu.org/en/post/exodus_static_analysis/.

Exodus Privacy (2020). What exodus privacy does. Available at: https://exodus-privacy.eu.org/en/page/what/.

Federal Assembly of Switzerland (2005). Tierschutzgesetz. Available at: https://www.fedlex.admin.ch/eli/cc/2008/414/de.

Federal Republic of Germany (2006). Animal welfare act. Available at: https://www.animallaw.info/statute/germany-cruelty-german-animal-welfare-act.

Fediaf (2021). Facts and figures 2020 european overview. Available at: https://www.nvg-diervoeding.nl/assets/files/fediaf-facts-and-figures-2020.pdf.

Gather Cover (2022). Pet theft in the UK, the stats and how to protect dogs and cats. Available at: https://gathercover.co.uk/guides/pet-theft/.

Giesbrecht, C. J. (2022). Animal safekeeping in situations of intimate partner violence: experiences of human service and animal welfare professionals. *J. Interpers. violence* 37, NP16931–NP16960. doi:10.1177/08862605211025037

Gittens, H. (2014). Man kills ex-girlfriend's dog, feeds it to her: cops. Available at: https://www.nbcnews.com/news/us-news/man-kills-ex-girlfriends-dog-feeds-it-her-cops-n202591.

Global Animal Law Association (2021). *Animal welfare legislation database*. Available at: https://www.globalanimallaw.org/database/national/index.html/.

Global Stats (2021). Mobile and tablet android version market share United Kingdom nov 2020 - oct 2021. https://gs.statcounter.com/android-version-market-share/mobile-tablet/united-kingdom/#monthly-202011-202110.

Global Stats (2022). Android version market share worldwide jan 2021 - jan 2022. Available at: https://gs.statcounter.com/os-version-market-share/android.

Government of Austria (2004). Federal act on the protection of animals (animal protection act – tschg). Available at: https://www.globalanimallaw.org/downloads/database/national/austria/erv_2004_1_118.pdf.

Government of the Netherlands (2011). Animals act. Available at: https://wetten.overheid.nl/BWBR0030250/2013-01-01.

Government of the United Kingdom (2006). Animal welfare act 2006. Available at: https://www.legislation.gov.uk/ukpga/2006/45/contents.

Government of the United Kingdom (2007). Welfare of farmed animals (england) regulations 2007. Available at: https://www.legislation.gov.uk/uksi/2007/2078/contents.

Grand View Research (2020). *Pet wearable market size, share and trends analysis report by technology (RFID, GPS, sensors), by application (identification and tracking, medical diagnosis and treatment), by region, and segment forecasts, 2020 - 2027. Grand view research*, Available at: https://www.grandviewresearch.com/industry-analysis/pet-wearable-market.

Groß, T., and Groß, T. (2017). Why privacy is all but forgotten. *Proc. Priv. Enhancing Technol.* 2017, 97–118. doi:10.1515/popets-2017-0040

Guhr, N., Werth, O., Blacha, P. P. H., and Breitner, M. H. (2020). Privacy concerns in the smart home context. *SN Appl. Sci.* 2, 247–312. doi:10.1007/s42452-020-2025-8

Harper, S., Mehrnezhad, M., and Leach, M. (2022a). "Are our animals leaking information about us? security and privacy evaluation of animal-related apps," in 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (IEEE), 38–51.

Harper, S., Mehrnezhad, M., and Mace, J. (2022b). User privacy concerns in commercial smart buildings. *J. Comput. Secur.* 30, 465–497. doi:10.3233/jcs-210035

Harper, S., Mehrnezhad, M., and Mace, J. C. (2020). "User privacy concerns and preferences in smart buildings," in International Workshop on Socio-Technical Aspects in Security and Trust (Springer), 85–106.

Information commissioner's Office (2021). Consent. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/#::text=Consent%20must%20be%20freely%20given,understand%2C%20and%20user%2Dfriendly.

Kohnfelder, L., and Garg, P. (1999). The threats to our products. Available at: https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx.

Levina, A., Varyukhin, V., Kaplun, D., Zamansky, A., and van der Linden, D. (2021). A case study exploring side-channel attacks on pet wearables. *IAENG Int. J. Comput. Sci.* 48, 878–883.

Martínez-Pérez, B., De La Torre-Díez, I., and López-Coronado, M. (2015). Privacy and security in mobile health apps: a review and recommendations. *J. Med. Syst.* 39, 1–8. doi:10.1007/s10916-014-0181-3

Mehrnezhad, M. (2020). "A cross-platform evaluation of privacy notices and tracking practices," in 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (IEEE), 97–106.

Mehrnezhad, M., and Almeida, T. (2021). "Caring for intimate data in fertility technologies," in Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 1–11.

Mehrnezhad, M., and Almeida, T. (2023). *My sex-related data is more sensitive than my financial data and i want the same level of security and privacy": user risk perceptions and protective actions in female-oriented technologies. arXiv preprint arXiv:2306.05956*.

Mehrnezhad, M., Coopamootoo, K., and Toreini, E. (2022a). How can and would people protect from online tracking? *Proc. Priv. Enhancing Technol.* 1, 105–125. doi:10.2478/popets-2022-0006

Mehrnezhad, M., Shipp, L., Almeida, T., and Toreini, E. (2022b). Vision: too little too late? do the risks of femtech already outweigh the benefits? *Proc. 2022 Eur. Symposium Usable Secur.*, 145–150. doi:10.1145/3549015.3554204

Miller, E., and McCaw, B. (2019). Intimate partner violence. *N. Engl. J. Med.* 380, 850–857. doi:10.1056/nejmra1807166

Moniz, D. M., Mehrnezhad, M., and Almeida, T. (2023). "Intimate data: exploring perceptions of privacy and privacy-seeking behaviors through the story completion method," in Proceedings of the 19th International Conference INTERACT 2023 (Springer LNCS). inpress.

Mozilla (2018). Mozilla *privacy not included. Available at: https://foundation.mozilla.org/en/privacynotincluded/categories/pets/.

Mutchler, P., Doupé, A., Mitchell, J., Kruegel, C., and Vigna, G. (2015). "A large-scale study of mobile web app security," in Proceedings of the Mobile Security Technologies Workshop (MoST), 50.

PFMA (2021). *Pfma 2021 annual report*. Available at: https://pfma-reports.co.uk/.

Prasad, A., Ruiz, R., and Stablein, T. (2019). "Understanding parents' concerns with smart device usage in the home," in International Conference on Human-Computer Interaction (Springer), 176–190.

Privacy International (2018). How apps on android share data with facebook. Available at: https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf.

Prolific Team (2022). What are the advantages and limitations of an online sample? Available at: https://researcher-help.prolific.co/hc/en-gb/articles/360009501473-What-are-the-advantages-and-limitations-of-an-online-sample-h.

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., et al. (2018). "Apps, trackers, privacy, and regulators: a global study of the mobile tracking ecosystem," in The 25th Annual Network and Distributed System Security Symposium (NDSS 2018).

RCVS (2018). Gdpr - rcvs information and q&as. Available at: https://www.rcvs.org.uk/document-library/gdpr-rcvs-information-and-qandas/.

Research and Markets (2019). *Global veterinary wearable devices market size, market share, application analysis, regional outlook, growth trends, key players, competitive Strategies and forecasts, 2018 to 2026*. Research and markets. Available at: https://www.researchandmarkets.com/research/xfkc78/global_3_7_bn?w=5.

Sinha, S. (2023). Iot connections market update—may 2023. Available at: https://iot-analytics.com/number-connected-iot-devices/#:~:text=The20endpoints.

State of California Department of Justice (2018). California consumer privacy act of 2018. Available at: https://oag.ca.gov/privacy/ccpa/regs.

State of California Department of Justice (2020). California consumer privacy act of 2018 amendments. Available at: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-add-adm.pdf.

Statista Research Department (2022). Mobile android os market share in the United Kingdom (UK) from 2017 to 2021. version. Available at: https://www.statista.com/statistics/1185416/mobile-android-market-share-version/.

Swedish Ministry of Trade and Industry RSL (2018). Animal welfare act. Available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/djurskyddslag-20181192_sfs-2018-1192.

Tabassum, M., Kosinski, T., and Lipford, H. R. (2019). "I don't own the data": end user perceptions of smart home device data practices and risks," in Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019), 435–450.

Taher, R., Mehrnezhad, M., and Morisset, C. (2020). "I feel spied on and i don't have any control over my data": user privacy perception, preferences and trade-offs in university smart buildings," in International Workshop on Socio-Technical Aspects in Security and Trust (Springer), 85–106.

The World Organisation for Animal Health (OIE) (2021). Terrestrial animal health code. Available at: https://www.oie.int/en/what-we-do/standards/codes-and-manuals/terrestrial-code-online-access/.

Tracki (2022). Tracki gps - track cars, kids, pets, assets and more. Available at: https://play.google.com/store/apps/details?id=com.trackimo.android.tracki\&hl=en_GB\&gl=US.

Turan, M. S., McKay, K., Chang, D., Bassham, L. E., Kang, J., Waller, N. D., et al. (2023). Status report on the final round of the nist lightweight cryptography standardization process

Vailshery, L. S. (2022). Number of iot connected devices worldwide 2019-2021, with forecasts to 2030. Available at: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/#:text=The%20number%20of%20Internet%20of,around%205%20billion%20consumer%20devices.

Vallina-Rodriguez, N., Sundaresan, S., Razaghpanah, A., Nithyanand, R., Allman, M., Kreibich, C., et al. (2016). *Tracking the trackers: towards understanding the mobile advertising and tracking ecosystem. arXiv preprint arXiv:1609.07190*.

Van der Linden, D., Edwards, M., Hadar, I., and Zamansky, A. (2020). Pets without pets: on pet owners' under-estimation of privacy concerns in pet wearables. *Proc. Priv. Enhancing Technol.* 2020, 143–164. doi:10.2478/popets-2020-0009

Van der Linden, D., Williams, E., Hadar, I., and Zamansky, A. (2019a). *Some might freak out: what if your dog's activity tracker were to have a data breach?* New York, NY, USA: Association for Computing Machinery), ACI'19. doi:10.1145/3371049.3371057

Van Der Linden, D., Zamansky, A., Hadar, I., Craggs, B., and Rashid, A. (2019b). Buddy's wearable is not your buddy: privacy implications of pet wearables. *IEEE Secur. Priv.* 17, 28–39. doi:10.1109/msec.2018.2888783

Wolford, B. (2019). What are the gdpr consent requirements? Available at: https://gdpr.eu/gdpr-consent-requirements/.

World Animal Protection (2021). Animal protection index. Available at: https://api.worldanimalprotection.org/.

Zarandy, A., Shumailov, I., and Anderson, R. (2020). *Hey alexa what did i just type? decoding smartphone sounds with a voice assistant. arXiv preprint arXiv:2012.00687*.

Zeng, E., Mare, S., and Roesner, F. (2017). End user security and privacy concerns with smart homes. *SOUPS*, 65–80.

Zheng, S., Apthorpe, N., Chetty, M., and Feamster, N. (2018). User perceptions of smart home iot privacy. *Proc. ACM Human-Computer Interact.* 2, 1–20. doi:10.1145/3274469