On the Security and Privacy of Animal Technologies

Scott Harper

PhD Thesis

Department of Computer Science
Newcastle University
Newcastle Upon Type, UK
March 2025

Abstract

As the Internet of Things (IoT), smart devices, and their corresponding mobile apps are becoming increasingly widespread, they are expanding into various different industries. One of these rapidly expanding sectors is animal technologies, which includes systems and devices designed to assist with animal care. In pet tech only, it is projected to reach a market value of $3.7 billion by 2026 [104]. However, these systems bring new security, privacy, and safety risks to users, their animals, and their homes. Despite these concerns, the risks of these systems, as well as the users' apprehensions about these issues, remain under-researched. This lack of research and data protection regulations in this space leaves users vulnerable to attacks and hampers their ability to protect themselves effectively. This PhD work investigates various aspects of the security and privacy of these technologies to inform the current state of risk and user perceptions.

Security and Privacy of Animal Apps: In the first part of this thesis, our work involves a range of tools used to perform static, dynamic, network traffic, and privacy policy analysis on a set of 40 animal Android apps (both farm animals and pets). We identify poor security and privacy practices that do not effectively gain the consent of the user and communicate their details in ways that may leave them vulnerable. We additionally find that some of the apps are communicating the user's login details in plaintext in non-secure http traffic, leaving them vulnerable to very obvious, yet dangerous attacks, by anyone who is able to view this network traffic. These issues were communicated to the companies responsible, with those who responded having the issue fixed upon later retesting.

Sensor-based IoT Identification: The second part of the thesis looks at a possible identification method to be used by resource-constrained IoT devices, with limited interaction methods, such as those used on and around animals e.g., at a large scale on a farm. In our proof-of-concept implementation, by utilising the accelerometers already present in such devices (i.e., the Nordic Thingy 52 and 53), we capture the data pattern created from physically tapping two IoT devices together. Our results showcase the feasibility of implementing such a system that is able to correctly identify matching tapping events from IoT devices which want to pair for secure communication. We test a range of signal processing methods, such as the correlation coefficient and energy of the signals, combining those found to be effective for our final similarity

calculation. The proposed system is able to achieve an EER of 3.5% when comparing 100 samples of data against each other, with possible adjustments to the threshold to get a lower FAR if needed.

User Studies of Animal Technologies Security and Privacy: In this final part of this PhD work, we turn our focus to the users of these systems (more specifically, pet owners). We design a user study in the form of an online survey to understand their views, concerns, and actions regarding these systems. Using Academic Prolific, we distribute this to 593 participants from the UK, US, and Germany (roughly 200 from each) targeting specifically pet owners. This study gives insight into the apps and devices used by pet owners, the perceived advantages and disadvantages, concerns, incidents that have occurred, as well as the different perceptions around the data that may be collected by them and how they might protect themselves from these risks. Despite only a few reported incidents with these technologies, we find 521 of the participants expressed concern about an incident, such as a data leak, and the well-being and safety of their pet. Despite these concerns, these participants took far fewer precautions toward protecting the security and privacy of these systems compared to what they employ for their general online security and privacy.

The findings of this PhD research give perspective to the overall security and privacy of animal technologies. Our work contributes to the body of knowledge in a holistic and comprehensive way, i.e., regulations review, system studies, secure system design, and user studies. We provide discussions and recommendations for multiple stakeholders such as academic and industrial researchers and designers, farm owners and managers, policymakers, and the end users of animal technologies.

Acknowledgements

I really couldn't have asked for a better PhD supervisor. Dr Maryam Mehrnezhad was nothing but supportive throughout the entire process, pushing me to work harder and push past the many little challenges encountered. Our regular meetings provided those extra boosts of motivation and reassurance that the project was moving in the right direction. This support continued despite Maryam's moving to Royal Holloway and was a massive help throughout the PhD. Her expertise in a range of security and privacy topics, including emerging technologies and sensors, helped inform and solidify the projects within my thesis. This expertise helped to guide and push me in the right direction when researching unfamiliar areas. Maryam's CyberMi2 Research Days were fantastic opportunities to attend, giving me more presentation, networking, and round-table discussion experiences. Her insistence on focusing on getting papers published based on my work proved to be an incredibly useful strategy, giving structure to how I went about completing this PhD project and thesis and providing me with the opportunity to attend multiple workshops and conferences. Thank you for all your help throughout my PhD project and my work outside of this. You really went above and beyond your expectations as a supervisor, I cannot thank you enough.

I would also like to thank my second supervisor Dr Matthew Leach. Though our contact was less frequent, Matt's support and insights into the animal and farm sides of the project were invaluable. His knowledge and connections helped to quickly gain an understanding of animal technologies and how they are actually used. Thank you as well for your help with my papers and this thesis, providing an alternate point of view outside of Computer Science.

Finally for my supervisors, I would like to thank Dr Charles Morisset, who stepped in and worked alongside Maryam and Matt, after Maryam's move to Royal Holloway. This made the transition seamless and prevented any setbacks in my work. Thank you as well for including me in your Smart Infrastructure group, where I was able to practice presenting and get feedback on the direction of my work.

Dr Danté Gray, a fellow PhD student at the time, was an immense aid in helping me settle into my PhD position and for setting an example of how I should carry out my research. His insights and assistance were a massive help in working with MATLAB, a system I had no experience with prior to this project. Congratulations

again on your recent graduation.

A particularly exciting part of this project was the press release and media interest that followed. This would not have been possible without the help of Newcastle University, and particularly Ivan Lazarov (Media Relations Manager). Ivan's assistance during this process, which I had no prior experience with, made things incredibly simple. I am incredibly grateful for the assistance and mock interviews Ivan provided, prepping me for the multiple interviews I would go on to have.

I would like to thank James Standen, the director of Newcastle University's farms. His information on the technologies in use and people to contact helped shape the early stages of the project, with him also allowing us access to some of the systems in use by the university. Our visit to the farms with him provided additional context into how the technologies are implemented and the vulnerabilities/threats they may face.

I would also like to thank the companies who responded to our messages informing them of the vulnerabilities found within our first project. These two companies expressed interest in finding out more about how they could fix the issues found, with these apps no longer presenting the vulnerability when later retested.

Finally, I would like to thank my friends and family for their support of me throughout the process. From getting me out of the house to helping trial my experiments, their help has been vital.

Being able to move back home during my first year and the COVID lockdown pandemic helped immensely in allowing me to properly concentrate on making a solid start to my PhD. I would like to thank my family, and parents in particular, for their constant support throughout my life and for providing the opportunities that have gotten me to where I am now. From my mum's constant support and pushing me to try things, to my dad giving up his days off to help me move, I couldn't have done this without you.

I would like to thank Mama (my grandma) for our lunches at Wetherspoons whenever I was back home, giving me a break from my research, and for her messages checking in on me when I was away.

I would also like to thank my family's dogs Alfie and Barney for not making too much of a fuss when I tried some of the activity monitors/GPS trackers on them.

I would like to thank my friends Katie and Pete. From living with you guys during my Undergraduate and Master's, where I first worked on the smart building privacy project that would go on to be my first published paper, to regularly popping around yours or chatting and playing online during my PhD, you two have always been there for me. Congratulations again on the wedding.

Thank you as well to my friend Nim, who has been a constant source of support throughout my time at university and beyond. You've seriously helped me more times than I can remember. Our various catch-ups and lunches throughout the years were always something to look forward to, along with the game nights around yours and Dave's. Thank you for always being there.

I would finally like to thank my friends from Undergraduate Computer Science. Though I regrettably didn't spend much time with you guys during Undergrad, I will be forever grateful for my inclusion in your Friday nights out during my PhD. Thank you to Matt, Cane, Zach, Nastya, Adam, Lindsey, and Rob.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

As the demand for animal technologies increases by end-users, for both farm [12] and pets [104], these industries offer more solutions that are potentially not secure. This is especially concerning for the farming sector, a critical national infrastructure in any country [4], that, given its importance, may be the focus of future attacks. Despite the smaller, more personal scale of attacks on pet technologies, their lack of security and privacy considerations are also concerning. Pet theft has reportedly increased over the past year, which can have an undeniable emotional impact on their owner [111] and may put those who rely on their pet, such as people with special needs who have an animal aid at risk. Hence, comprehensive research is required to assess and analyse the current security and privacy practices of technologies present in these industries to protect the users of these systems. Table 1.2 shows examples of possible cyber-attacks on these systems which can potentially affect the animal, owner, farm, and wider society.

The research in this area is sparse and only a few previous works have addressed the security and privacy issues of animal technologies [9, 132]. We look to address the research gap of this growing area of technologies by analysing a range of security and privacy aspects surrounding these technologies. This work looks to identify current issues and concerns, as well as, desired protection methods and possible solutions for secure identification and authentication within low-powered IoT devices.

1.1 Animal Technologies

Smart devices for animals are becoming increasingly popular. Veterinary wearables are expected to reach a market value of $ 3.7 billion by 2026 [104] and pet wearables had a market size valued at USD 1.6 billion in 2019 [99], with multiple devices even

		
Activity Monitor Communicates data via Bluetooth to an app on button press.	**GPS Tracking Device** Constant access to GPS data, Accessed via app, Uses SIM card to connect to networks.	**Automatic Feeder** Smart feeders operate using an app, Connects to WiFi.
		
Pet Camera Access via app, Data stored on the cloud, Can capture audio, have nightvision.	**Activity Monitoring App** Contains personal information, Share activity with others, Receives data from device or server.	**Automatic Ball Launcher** Can allow dogs to play by themselves, Some may be operated using a remote

Table 1.1: Examples of pet technologies used by the participants of the study

appearing in adverts on UK television. Kippy, a pet wearable company whose app is studied in this thesis, has more than 17,000 active users and was expected for this to increase to 300,000 by 2023 [50]. Fediaf, the European pet food industry, reported the annual sale of pet accessories in 2020 as being 9.2 million [31]. Given the 2.8% annual growth of the pet food industry in 2020 [31] and the recent increase in pets in countries such as the UK (11% of households acquired a new pet) [79], these sales are likely to grow as more people own pets and begin to adopt these technologies.

These pet wearables can have a variety of features, such as activity monitors that work as a sort of Fitbit[1], tracking a pet's exercise and when they are active, e.g., PitPat[2]. Another type of these devices includes GPS tracking, giving the exact location of the animal at a given time e.g. Tractive[3]. Pet tracking devices have been found to be used for other reasons including the tracking of children (e.g. the app "Trackimo GPS for child pet car" with more than 20K users so far[4]). This is specifically concerning since security and privacy regulations vary across the user groups [100], with various levels of protections. The legislation surrounding animals

[1] fitbit.com/global/uk/home
[2] pitpat.com/
[3] tractive.com/en/
[4] `play.google.com/store/apps/details?id=com.trackimo.app&hl=\en_GB&gl=US`

Table 1.2: Cybersecurity attack examples in animal technologies

Attack type	Farm animal	pet
Spoofing	Attacker uses a farmer's phished login details to gain access to their account [52]	Attacker accesses the user's account to access acount details or impersonate
Tampering	Manipulating environmental temperature to harm the poultry production [54]	Manipulating the feeding/medicine system to harm pets [9]
Repudiation	Deny altering animal health records [113]	Deny ownership of an abandoned pet [58]
Information Disclosure	Stealing the herd health data to damage finance/reputation [2]	Stealing pet microchip information e.g. address & GPS [129] for spamming/phishing attacks
Denial of Service	Service interruptions on remote access tools [119]	DoS/ransomware attacks to prevent a lost pet being found
Elevation of Privilege	Attacker becomes an admin and removes animals from an online farming system [52]	Access to and ability to alter owner and pet details

and their data will be discussed later. Examples of these pet devices can be seen in Table 1.1.

Furthermore, these types of technologies are now increasingly being used by the farming industry [12]. We refer to these technologies used on farm animals as **Agritech**. Herdwatch, iLivestock, Digitanimal, and Fullwood Packo are used by over 10,000, 5000, 3,800, and 50,000 clients/farms respectively [47, 48, 22, 93]. This agritech industry is continuing to grow, with companies like Gea (FarmView) seeing an 18.4% increase in farming technology order intake and a 1.8% increase in revenue, with this being the only area of their business seeing a growth in revenue between Q2 2020-2021 [33]. Lely also saw growth last year, with an increase of sales from €606 million to €615 million [56]; along with DeLaval, which saw a 20% increase in the sale of their milking robots [21]. These companies anticipate even more growth in this industry, with Gea seeing an increase in revenue of €42 million from their previous financial year[5] and smaXtec aiming for 1 million cows being monitored by their systems [118]. As seen by these statistics, technologies for both farm animals and pets are growing industries seeing new devices and types of devices becoming available to consumers. These devices are collecting information about the people interacting with these animals, as well as their environment, in new and different ways. The apps of all the above mentioned companies are studied within this work.

1.2 Potential Risks

1.2.1 Agriculture sector

Cyber-attacks against critical national infrastructures are an ever-growing threat to countries, with a variety of national infrastructures being targeted. These past attacks have targeted infrastructures such as sewage plants (Maroochy Shire 2000) [3], electrical grids (Ukraine 2015) [13], water treatment plants (Israel 2020 [77], Florida 2021 [124]), nuclear plants (Iran 2010) [30], and healthcare systems (UK 2017) [34] and can have disastrous consequences, endangering the lives of those affected.

The agriculture sector is an integral part of any country, being regarded as the economic backbone of developing countries [117] and is considered by many governments as a critical national infrastructure [4]. The implementation of IoT technologies within this sector will enhance its capabilities through increased efficiency and is being seen as the 4th industrial revolution [105]. However, with the increased use of IoT in this sector, it becomes more vulnerable to attack due to the increased attack surface [9, 14], introducing a range of potential internet connected devices collecting large amounts of data. One of the major concerns in IoT is the possibility for unsafe mobile interfaces [116] that may expose users to an attack. This is a significant worry for the smart agriculture sector as farming systems become increasingly connected, with access to them typically being done through web applications such as FarmWizard[6], allowing for remote access to intimate details of how a farm is operating.

Another especially concerning vulnerability is the possibility of food supplies being tampered with by internet entities [4], potentially resulting in shortages or unsafe products. Even the smallest alterations to food production systems may have disastrous consequences, resulting in huge losses to a farm or potentially more fatal outcomes if consumed by humans [116]. Attacks on the agriculture sector will have a lasting impact on the consumers' trust resulting in significant financial consequences [14]. A cyber security threat analysis of the UK agriculture sector identified that there are threat scenarios that could lead to "significant harm to the industry, social unrest and suffering to livestock" [9]. Given the importance of this sector, and these possible vulnerabilities, data security is a top priority in IoT-based agricultural systems [116] and is an important area to study. Any new technologies being introduced into these environments must handle data securely to help protect against such severe

[5] cdn.gea.com/-/media/investors/annual-report/2023/annual-report-2023.pdf?rev=8969dee4aee84a1cadb9656a5fd6d0b4

[6] farmwizard.co.uk/

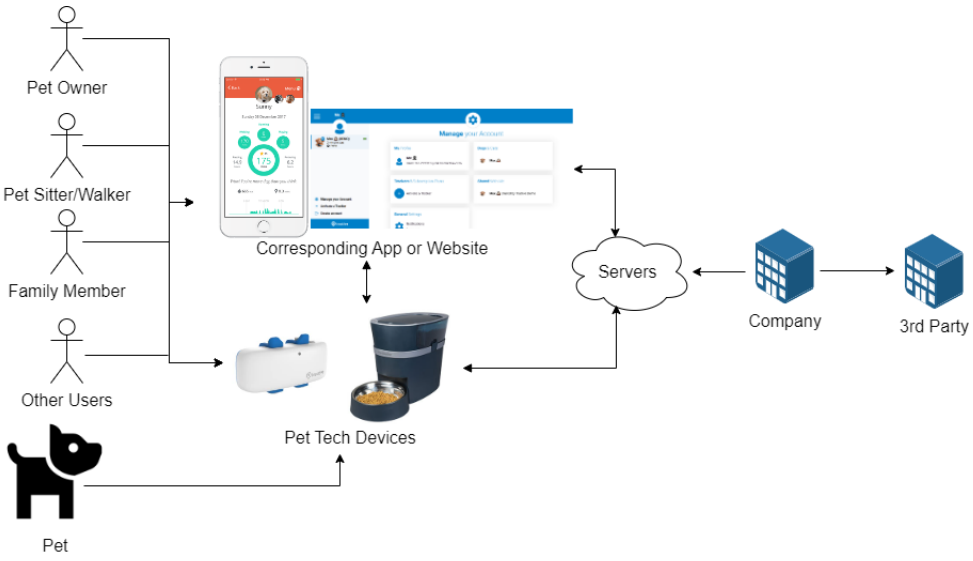

Figure 1.1: The Pet technology ecosystem; showing how users interact with these systems. Other users may include vets, insurance companies, health clinics, etc.

and potentially dangerous attacks.

1.2.2 Pet Tech ecosystem

Despite the smaller scope of people (per system) impacted by these devices and the data collected, they still affect a number of different people that would interact with or be around pets that are being monitored in some way by these devices, as shown in Figure 1.1. Children who help to take care of their family's pet or simply play with them may have data about them captured via environmental sensors or by directly interacting with the animal. Those hired to aid in the care of a pet, e.g., a sitter or walker may have data implicitly captured about them, or these devices may be used more directly to snoop on them.

There are additional marginalised groups who may rely on these devices. Those who are visually impaired or on the autistic spectrum may rely on a pet animal to support them. These groups may then utilise these pet tech devices to aid in the care of their support animals, leaving them potentially at risk. There is a similar case for the elderly or those who are physically impaired, who may rely on these new devices to help reduce the workload in caring for their pet or may turn to these devices to provide a sense of comfort in terms of the health of the animal and in preventing them from getting lost.

It is also possible that pet tech systems may potentially endanger women more than men. Multiple past studies have shown that women take on a greater amount

of household responsibilities [18][125]. Pet care may be one of these responsibilities, making women be more likely to interact with these pet technologies compared to men. There have also been multiple instances of ex-partners using pets as a means of revenge against women in pretty gruesome ways[7] [8]. Introducing additional data collecting devices may further enable or escalate these attacks against women who own pets.

1.2.3 Possible attacks

Despite the benefits, as with other IoT technologies, these devices and applications add an extra opportunity for security risks. The data collected and held may be sensitive and may potentially be used by an attacker to exploit the user. Even the leak of less sensitive personal details may enable further attacks such as phishing. Previous work such as [127] show that various IoT systems can be vulnerable to a variety of attacks. Pet devices and applications capture data that may give insight into their users' routines and location and it has been shown that more data is captured about the users than their pets [132]. With these devices capturing data around the interactions or environments of these animals, it potentially also puts at risk all those interacting with these animals, not just the main user, as mentioned in Section 1.2.2.

Data captured from farm animals could inform the attacker on how a farm operates and may be taken out of context and used to potentially blackmail or damage a farm's reputation, a concern that was particularly highlighted when discussing IoT risks with the industry (pers comm). These attacks are made more likely given that a higher number of users within an IoT system, like on a farm, leads to the increased vulnerability of an IoT system [80], with more avenues for attack.

As can be seen in Table 1.2, various forms of cyberattacks can potentially affect the animal, owner, farm, and wider society if there are no security and privacy features in place in the design and implementation of these systems. In this table we use the STRIDE model [52], a security model designed to help anticipate the different cyberattacks that may be possible against a system, to demonstrate a variety of possible attacks. Here we give examples of possible attacks that may be undertaken against both pet tech and agritech technologies.

Spoofing, in the STRIDE model, refers to when an attacker is able to claim that they are someone that they are not within the system [133]. In the case of farm animal systems, this could involve an attacker gaining access to a farm's account

[7] nbcnews.com/news/us-news/man-kills-ex-girlfriends-dog-feeds-it-her-cops-n202591
[8] mirror.co.uk/news/uk-news/jilted-boyfriend-took-revenge-ex-5393743

and then interacting with the system or other users. A similar attack may be done on the account for a pet wearable or any other wearable devices. In this case, the attacker would able to view account details, potentially including GPS data, showing past walking routes and, again, would be able to interact with others within the app, impersonating the actual user.

Tampering is where an attacker is able to alter the data within the system in some way, causing the data to be unreliable. In a farming system, this may mean an attacker that is able to change the temperature in rooms where animals are kept, possibly affecting their growth [54] or causing heat stress [139]. Similarly, pet feeding machines, which can also be used to dispense their medication, may be prevented from giving the food and/or medicine to the pet, causing them harm [9]. An attacker may also be able to spoof the GPS data, feeding the user incorrect GPS information to prevent them from locating the tracking devices (and the animal it is attached to). This would enable further attacks/exploits, aiding with animal theft or to potentially gain money from the owner.

Repudiation is the ability for a user to deny something that they have done. For a farming system, this may mean an untrustworthy farmer is able to deny altering an animal's health record, hiding past treatments and illnesses, to make it seem healthier than it is. This could be done to increase the value of an animal or to falsely pass a health inspection. A pet owner, on the other hand, may try to claim that an abandoned pet is not theirs.

Information Disclosure is where the attacker is able to gain access to information that they should not be able to. As mentioned before, a major concern for farmers is the possibility of their herd health data being stolen, with this potentially being used by their competition, or to damage their reputation [2]. For pet technologies, this information could be user address information from their pet's microchip or GPS [129] and further user information from a pet wearable/app.

A **Denial of Service** attack prevents a user from accessing or using a system. For farmers, this may mean that they are unable to use their remote access tools [119] and may prevent them from spotting an animal with a health condition, if they are reliant on a system to do this. The attack could also be used to intentionally prevent a lost pet from being found by not allowing the system/user from receiving the pet's location information. This may be done to try and gain money from the user or to aid in pet theft, which is becoming increasingly commonplace [111].

Elevation of Privilege is where an attacker can not only claim to be a valid user but one with expanded privileges, e.g., an admin. This would be very dangerous in an

online farming system, where someone with administrator privileges has the ability to remove animals from the system and potentially also affect their environment. Administrator-type roles are not as common in pet wearable systems, however, may exist in applications designed to be used with a dog walker or pet sitter, who should not have access to all of the features, and may become more common in the future. In this case, an attacker would be able to get access to owner and pet details and be able to alter these in some way.

1.3 Research Questions

This work aims to analyse the security and privacy of the technologies used with farm and pets. Despite these technologies becoming more commonplace, little research has been done into this research area. The main goals of this project are to demonstrate whether these technologies used with animals are secure and respect the users' privacy, and if not, how these issues can be fixed. Our specific research questions are as follows:

RQ1. Are animal technologies secure?
Through carrying out this research, the first goal is to identify what technologies are actively being used both in farms and for pets. For the farming systems, those used by Newcastle University Farms will be looked at due to having access, a selection of other popular farming apps will be looked at as well. Pet technologies will be selected based on their availability in shops and their popularity in the case of app downloads. Further details on this selection process are provided in Section 3.3.1.

A different online system is needed for pretty much every device used by farms, all of which may be vulnerable and potentially accessed by an attacker. Some of these online systems have an app to access them and pet devices all have their own app. It is possible that these apps may not communicate personal information securely and may reveal user information including their login details during the user's authentication.

The possible privacy issues centre around the applications and online systems attached to these animal technologies. These apps may send user information, such as login details, to other companies not associated with the app. As well as this, apps may use tracking services before checking whether this is okay with the user. Privacy policies are another possible area of issue, with these applications potentially not adhering to the GDPR in the way that they present their privacy policy to the user if they present one at all.

RQ2. Can secure solutions be developed for these technologies?
To fix bad app practices, the companies responsible for any systems found to have issues will be contacted. This includes those who design the apps studied, particularly any apps presenting serious security vulnerabilities. In the short term, this should help protect users by removing the currently present vulnerabilities putting them at risk. In the long term, making companies aware of the vulnerabilities present in their systems, and the risks associated with them, should help to underline the importance of considering the security of their systems. This will hopefully result in the development of more secure systems in the future.

Looking at the actual devices being used, work will be done on a secure and easy-to-use identification mechanism for connecting IoT devices to a system, contributing to a more secure authentication mechanism. This system, which would involve tapping devices together may be applied to animal wearables to provide a simple to set-up system for those with limited technical experience. Making use of the already present motion sensors common within animal technologies will allow for a system that can function with devices that are otherwise lacking in input methods, e.g., no touchscreen or buttons. We focus on the initial identification and authentication of these systems given the security flaws identified within our app study, showing that this is an area lacking in adequate security design.

Any solution proposed must effectively protect the user, by detecting invalid connection attempts. As such, this identification mechanism must have a low FAR (false acceptance rate), with this being the priority of the system. The potential trade-off here is the FRR (false rejection rate), how likely a valid user is to be rejected by the system. Whilst a lower priority, it is still important for this metric to be low in any proposed identification, and subsequent authentication system, so that the system remains usable.

RQ3. How aware are the users of these technologies and what are their concerns?

It is important to know whether those who use these technologies are concerned about their security and privacy, alongside their awareness of possible issues in this area, as well as their current security practices. User studies of farm and pet technology users would allow for this information to be collected, allowing for more informed recommendations and design of secure, privacy-preserving technologies that users can feel confident in using.

The results of the user study will help give an insight into the concerns of those

actually interacting with these devices/systems. This should then help in the design of future studies in this area and aid with the design of future best practices. This will allow for the design of more secure and usable systems in the future.

1.4 Summary of Contributions

Within this work, we aim to cover a range of aspects relating to animal technologies and their security and privacy. This PhD project has three specific contributions: (1) a series of system studies and attacks performed on a list of animal apps, in addition to a legislation review, (2) a secure pairing system design implemented on IoT sensors, tailored to animal technologies and applications, and (3) user studies across three countries (UK, US, and Germany) to understand the concerns and protective actions.

We first review the literature on animal technology security and privacy, looking at the research that has already been completed in this field and the areas that they cover. Given the limited amount of research that has been completed, due to this being a relatively new area of technology, we also review the literature of adjacent research fields. These other areas include the research around the security and privacy of different smart device contexts as well as more general applications.

In addition to our review of the literature, we also conduct a review of top-ranking animal welfare legislation, to see if these smart technologies, or the data they captured are referenced or covered in any capacity.

We then begin our analysis of the animal technologies, focusing on the apps that interact with them. Looking at the 40 most popular Android apps (20 pet, 20 farm), we employ a range of methods and tools to identify serious security vulnerabilities and poor privacy practices within this set of applications. We find that three of the apps are communicating the user's login details in a very insecure manner, leaving them vulnerable to a simple interception attack. This vulnerability was reported to the companies responsible, after which, this vulnerability was no longer present in the two apps whose company responded to us. We also highlight the range of poor privacy practices present within the animal app ecosystem, of which, very few respect their user's privacy.

After identifying poor security practices in the apps associated with these devices, we propose a potential method for authenticating resource-constrained IoT devices, with limited interaction methods, such as those that may be used on or around animals. Due to the necessary physical robustness of these devices, they often lack touchscreens or other methods that may be used to enter a password. Instead, we look

to make use of the already present motion sensors (in this case the accelerometer) to generate a shared piece of knowledge between two devices that are tapped together.

Using IoT prototyping platforms (Nordic Thingy 53), we are able to achieve an EER (equal error rate) of 3.5% when comparing 100 samples of tapping data and compare these results to related authentication and fingerprinting research. This proposed identification may be implemented to allow for a usable and secure authentication system. We additionally discuss possible improvements and areas of research that may be investigated, including the addition of other sensors, testing this system with varied device types, and fingerprinting users.

Following on from these two studies, we then turn the the user's perspective, investigating: 1) Their reasons for use, perceived advantages, and disadvantages, 2) Any incidents that have occurred relating to the devices they use, 3) Any incidents they believe may occur as a result of using these technologies, 4) Who they believed would be responsible for an attack, 5) The protective actions they take both generally and for the pet technologies they use, with regard to their security and privacy, 6) Their desired protective measures and who they think is responsible for ensuring the security and privacy of these technologies.

We distribute this user study to just under 600 participants from three different countries (UK, USA, Germany). Our results show that concerns are present among those using these technologies, typically less so around their own security and privacy and more about the safety of their pets. However, despite these concerns being present, the participants stated that they took far fewer precautions to protect their security and privacy when using these technologies, compared to their general precautions taken in other scenarios, e.g., online.

We evaluate and compare the results of our studies, seeing if the users' awareness, concerns, and actions reflect the reality of the security and privacy of pet technologies. From this, we make recommendations for the various stakeholders involved within the animal tech ecosystem to try and better protect those who may be interacting with these devices.

1.5 Thesis Outline

Chapter 2: Background and Related Work. This chapter introduces a range of related studies that provide context and inspiration for the projects within this work. We first look at papers focused on the use of technologies used on and around animals in a farming environment. We then look specifically at security and privacy

studies of animal technologies (farm & pet tech). Given the limited work in this previous area, we additionally cover IoT security and privacy around different types of technologies, such as those designed around humans. Accompanying this, we cover studies looking at smart building security and privacy for works focusing a bit more on environmental monitoring. We then look at security and privacy studies on apps, providing background for our 1st project. Finally, we cover the related works for a sensor-based identification method before moving on to the next chapter.

Chapter 3: Security and Privacy of Animal Apps. This chapter's focus is on the methods and results of the first project in this work [42]. We provide a brief review of the current legislation surrounding animals and data captured about them. Then move on to study the security and privacy of farm and pet-based apps available to consumers. Using static, dynamic, network traffic, and privacy policy analysis methods, we identify a range of flaws in how these applications are designed.

Chapter 4: Sensor-based IoT Identification. This chapter covers the processes and results of our second project, focusing on a potential identification method for low-powered IoT devices with limited interaction methods (such as those used on animals), for use in an authentication system. This covers the devices and methods used, the data collection methods employed, and the effectiveness of the proposed solution. Looking to make use of the accelerometers available on many animal-based devices, the proposed identification system compares the motion data collected by two devices during a tapping event. We collect 10 samples per device from 25 different participants (250 tapping processes total) and test the applicability of such a system, calculating the equal error rate (EER).

Chapter 5: User Studies of Animal Technologies Security and Privacy. This chapter focuses on our third project within this work [43], covering our survey design and distribution as well as our findings. The focus of this study is the concerns and precautions taken by participants and their desired protective measures. We distributed this study to just under 600 pet owners, identifying a range of technologies being used, along with various concerns and misaligned security practices.

Chapter 6: Discussion. In this chapter, we summarise the results of our projects and discuss the overall implications of our findings across the various projects. This gives insight into how the views of actual pet owners and pet tech users compare

with the possible risks present within these technologies. Our projects motivate the need for a more security-focused mindset in the development of these technologies, showcasing one of many such possible solutions. We provide a range of recommendations that may help to protect the users of these animal devices, as well as other IoT products.

Chapter 7: Conclusion. This chapter provides an overview of the findings from the projects contained within this thesis. We additionally highlight some areas of possible future research based on the results of our work.

1.6 Outputs

PhD Publications. The list of my works that have been published throughout the duration of my PhD include:

1. Harper, S., Mehrnezhad, M. and Leach, M., 2022, June. 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) (pp. 38-51). IEEE[9].

   This publication covers the security and privacy of animal apps. This paper is mainly presented in Chapter 3 of this thesis.

2. Harper, S., Mehrnezhad, M. and Leach, M., 2022, November. Security and Privacy Concerns of Pet Tech Users. In Proceedings of the 12th International Conference on the Internet of Things (pp. 155-162)[10].

   A publication featuring the work of the user studies of this project. This is mainly presented in Chapter 5 of this thesis.

3. Harper, S., Mehrnezhad, M. and Leach, M., 2023. Security and privacy of pet technologies: actual risks vs user perception. Frontiers in The Internet of Things, 2, p.1281464[11].

   This journal publication expands upon our previous user study, whilst incorporating our app study, providing additional insights. This paper is presented in both Chapters 3 and 5 of this thesis.

[9] ieeexplore.ieee.org/abstract/document/9799417
[10] dl.acm.org/doi/abs/10.1145/3567445.3571102
[11] frontiersin.org/journals/the-internet-of-things/articles/10.3389/friot.2023.1281464/full

Other Publications. In parallel to my PhD research, I also worked on another project which contributes to the understanding of user studies of my PhD research.

4. Harper, S., Mehrnezhad, M. and Mace, J.C., 2020, September. User privacy concerns and preferences in smart buildings. In International Workshop on Socio-Technical Aspects in Security and Trust (pp. 85-106). Cham: Springer International Publishing[12].

   This work provides context into how people understand the smart environments and technologies that they interact with.

5. Harper, S., Mehrnezhad, M. and Mace, J., 2022. User privacy concerns in commercial smart buildings. Journal of Computer Security, 30(3), pp.465-497[13].

   These two papers provide context into how people understand the smart environments and technologies that they interact with.

Media Impact: This work (especially the app security aspects) gained international media attention after a press release from Newcastle University. It appeared in a physical copy of The Telegraph, as well as various online articles including The Express[14], Science Daily[15], The Star[16], and La Opinión[17]. Additionally, the work appeared in a brief video segment on CBS Miami[18] and led to interviews for podcasts (The Naked Scientist[19]) and online articles (IT Brew[20]).

Other Outputs.
Coursera Interview: As part of an online program on information privacy, I was interviewed for my expertise on smart buildings and pet tech privacy. This involved discussions around the surveillance present within these technologies and how users look to achieve privacy with the data involved in these systems. This was a part of the Royal Holloway Information Security Programme.

[12] link.springer.com/chapter/10.1007/978-3-030-79318-0_5
[13] content.iospress.com/articles/journal-of-computer-security/jcs210035
[14] google.com/amp/s/www.express.co.uk/news/science/1740442/dog-tracker-app-cyber-security-pets-study/amp
[15] sciencedaily.com/releases/2023/02/230227193312.htm
[16] thestar.com.my/tech/tech-news/2023/03/02/how-pet-related-apps-could-be-a-cybersecurity-risk-to-owners
[17] laopinion.com/2023/02/28/tu-mascota-podria-estar-filtrando-informacion-importante-sobre-ti/amp/
[18] cbsnews.com/miami/video/new-warning-about-using-pet-apps/#x
[19] thenakedscientists.com/articles/interviews/peoples-data-hacked-their-pet-apps
[20] itbrew.com/stories/2023/04/14/users-of-pet-tech-admit-to-slacking-on-security

CyberMi2 Research Day: The app and user study aspects of this work have been presented at both CyberMi2 Research Day events[21], in 2023 and 2024. Here the methods and results of these studies were discussed with members of the CyFer and AGENCY projects, both of which are EPSRC-funded research groups.

Round-Table Discussions: I also led a round table discussion on the security and privacy of animal technologies at the closing event of the CyFer art exhibit in 2023, partnered with EPSRC NCSC RISCS. We discussed possible ways to protect users of these technologies and how more general and all-encompassing legislation is needed to ensure the security of these newly developing areas of IoT devices. These discussions engaged participants from academia, industry, and the government, and helped inform our background, related work, and discussion.

[21] sites.google.com/view/maryammjd/cybermi2-2024

Chapter 2

Background and Related Work

This chapter covers the work related to agritech development studies, animal technology security and privacy, and other related security topics such as IoT, smart buildings, mobile app security and privacy studies, and sensor-based authentication systems.

2.1 Agritech Development Studies

We start this chapter by reviewing a selection of research on developing technologies for use on and around farm animals to highlight the development of these systems and the types of data that they may collect. Although these works do not focus on security and privacy, this section should give more context into the studies being done on technologies around animals. Given the range of proposed solutions for these problems, we do not cover specific technologies, e.g., experimental motion sensors for lameness detection, as these are not commonly deployed in the real world. Instead, we highlight the research around the development of these technologies, showing advancements and the types of research being performed, as well as the growing number of technical solutions being developed for this sector. Real-world examples of the types of technologies used on farm animals can be seen in Figures 2.1 and 2.2.

In an overview of the growing farm technologies [7], the authors of Agricultural Informatics discuss the various use cases of IoT on farms. Although mostly focused on crops, as opposed to animals, this book details the biggest obstacles when it comes to designing these technologies. These are as follows: the lack of smooth integration with the industry, a lack of an optimally skilled workforce, and a need for these devices to work wirelessly, consume low power, maintain connectivity, be secure, and allow for remote management [7]. Additionally, this work details some of the possible security

Figure 2.1: (Left) Cows wear devices on their collars that may collect (e.g., eating habits and rumination). (Right) Environmental sensors hanging above a sow and its piglets. Feeding technology and the living environments can be equipped with smart sensors connected to the internet. Images were taken during our visit to Newcastle University Farm, Dec 2020.

threats and concerns in using IoT on farms, with mentions of unsafe mobile/web interfaces, as well as the modification and leaking of data.

The collection of studies in the book: Precision livestock farming applications [41], covers a variety of different ways in which sensor-based technologies may be applied for use with farm animals. This set of previous studies includes categories such as 'Automatic Lameness Detection', and 'PLF for automatic detection of health in cows', where PLF stands for Precision Livestock Farming. The book provides a good summary of those works being conducted around the applications of technologies on farm animals for a range of applications, useful for those looking for an overview of the current research in this area. This book shows the extent to which sensor-based technologies can and may be used with farm animals, highlighting the growth of these technologies and the data they may capture.

In a study of the practical deployment problems of these technologies, Banhazi et al. deployed them on commercial farms and evaluated the issues and benefits [10]. In this large-scale trial of PLF technologies, they found 30 main deployment issues, including overheating, physical damage via animals, and unreliable connections that may be difficult to set up. This work emphasises the inherent difficulties and dangers in installing PLF tech.

Figure 2.2: (Left) Devices worn by cows attached to a collar. (Right) Cows with identification tags on their ears. Images were taken during our visit to Newcastle University Farm, Dec 2020.

Several studies have shown the possibility and further development of systems to manage and help maintain the health of farm animals. The work by Neethirajan et al. highlights the recent advances in this area with regard to wearable technologies [74]. They highlight a variety of the more advanced biosensors being studied, focused on areas such as sweat analysis, pathogen detection, stress detection, movement, and behaviour. This work shows the growth in research surrounding the development of these technologies and the likely subsequent commercial adoption.

Aside from the health management of individual animals, multiple studies focus on environmental sensors used in farm animal buildings suchas those in Figure 2.1 (right). These include temperature and gas sensors that maintain the safety of the animals. An example of this is the work by Mendes et al. shows a potential new gas sensor to allow for the measurement of carbon dioxide concentrations in naturally vented livestock buildings [68]. This new lower-cost method uses an infrared source and detector to ensure the air quality for farm animals.

In a study performed by Costopoulou et al., [20], the authors look at farm-based mobile apps and their development, being one of the few studies in this area. They find that there are a very small number of apps available in relation to the sector's significance, however, suggest that "mobile agriculture apps show significant potential for the modernization of the agriculture sector". This investigative work into the growth of agritech and corresponding apps, shows that despite limited apps being available at the time of the study, it is inevitable for their number to increase. With

Paper	Year	Agritech	Pet Tech	Security	Privacy	Focus
[4]	2017	✓	-	✓	-	Discuss need for security & possible risks
[130]	2020	✓	-	✓	✓	Data sharing practices of interviewed farmers
[131]	2020	-	✓	-	✓	User study of security and privacy concerns
[129]	2020	✓	-	✓	-	Analysis of product reviews
[57]	2021	✓	-	✓	-	Security vulnerability in dog tracker
[71]	2017	-	✓*	✓	✓	Consumer security & privacy guide
This PhD Project	-	✓	✓	✓	✓	Comprehensive approach i.e., system studies (attacks, design) and user studies

Table 2.1: Overview of security and privacy studies focusing on animal technologies. * Consumer devices and IoT, including some pet tech devices.

the growth of this area of apps, ensuring that they function securely and respect the user's privacy will be even more important.

The above studies show that a range of new technologies are being developed, similar to pet tech, for the use of data collection/management on and around farm animals. As these developments are integrated into the real world, a greater amount and more accurate data will be collected and likely stored for analysis. However, given the focus of these studies of solving these specific solutions, they do not focus on how to properly handle the data they output. We have already discussed the limited studies into the security and privacy of agritech systems, showing that there is no real focus on analysing and protecting these systems. The work within this thesis, looks make a start in this area, analysing the systems and users and offering a possible secure authentication solution.

2.2 Animal Technology Security and Privacy

Despite the growth of these markets and the popularity of these devices, as discussed in section 1.2, there is very little research into the security and privacy of these devices and the technologies surrounding them. This is especially the case for agritech, despite the potential implications of an attack on what is critical national infrastructure. We cover the limited research in this area, splitting the works into agritech or pet tech.

2.2.1 Agritech

As mentioned above, the amount of work around the security and privacy of the technologies and systems used on and around farm animals is particularly limited. Here we show the research that is available, which showcase some of the perceived vulnerabilities and avenues for future research.

Song et al. discuss the need for these technologies to be designed securely, as well as the current setbacks in achieving this, such as a lack of information being given to farmers [4]. This work makes an important step in this research, highlighting some of the possible threat models that may endanger those using IoT devices on farm animals. A big focus here is the misuse or misrepresentation of the collected data in some way, as well as the leaking of farm data, possibly as the result of political action or terrorism. In fact, in our discussions with the farm director of Newcastle Univeristy Farms, we saw a similar focus on this concern of data misuse/misrepresentation, with it being the main concern regarding the data collected by these Agritech systems. Recommendations are provided by the authors, including encryption of the data collected by the technologies and operational considerations such as data retention policies. The threats presented within this work show the necessity for these agritech systems to be designed securely and the need for further research into the security and privacy of these technologies to protect the end users.

Work by Van der Linden et al. discusses the effect of social-cultural context on cybersecurity in farming [130]. Their work covers the differences in vulnerabilities when technologies are used within different countries and doesn't focus on specific technological vulnerabilities/solutions. The study involved interviewing farmers in different countries, finding different data-sharing practices in the UK and Israel. The authors of the study believe these differences would impact the security and privacy needs of those farmers. For example, the farmers in Israel are already in the practice of sharing their farming information between themselves for the benefit of everyone. They would therefore be far less concerned about a data leak within an agritech system at the hands of a competitor, whereas for farmers in the UK, this leak may have a much more significant impact and be of a greater concern to them. This work showcases some of the perceived threats direct from farmers and how they may change within different cultures. This is an aspect that may be important to take into account when developing IoT systems that may be used internationally.

2.2.2 Pet Tech

One previous study by Van der Linden et al. has looked into the security and privacy concerns of dog owners that use one brand of activity tracker [131]. In this study, the authors ask 61 users of these devices about a hypothetical data breach and their concerns regarding this. They find a lack of concern amongst these users, especially regarding the privacy of the data collected via these devices. The few concerns they

do find, centre on the physical safety of their dog and others. Because of this lack of privacy concern and lack of awareness of the risks, the authors argue that owners should be better informed about the privacy implications of the activity data captured.

In another paper by Van der Linden et al. [129], focused on privacy risks and concerns, the authors perform a study looking at product reviews for pet technologies. In their analysis of over 8000 reviews, they find a lack of privacy concerns when using these technologies when compared to the reviews of human wearable technologies. The authors perform an additional survey targeted towards pet owners, finding similar levels of lacking privacy concerns among their participants, believing this to be the result of a more emotional focus of those purchasing these devices for their pets. Additionally, a particularly concerning discovery was made, that these devices are being used in different ways than intended, such as to track children, raising issues around the security and design process, as well as legislation.

In a prior study of wearable devices by Van der Linden et al., the authors focus on the data collected by these devices [132]. Comparing what these devices advertise to the reality of the data they capture, the authors find a mismatch, with some non-tracking devices actually tracking the user via the app. These misrepresentations, along with missing information regarding the storage of the data leave users of these devices unaware and uninformed of the possible privacy issues that may be present. The paper also discusses the classification of pet data, believing it should be viewed as personal data given the inevitable collection of the owner's data. Furthermore, the authors find that these pet technologies, and their corresponding applications, actually capture more data about the owner than the pet. This study highlights that these technologies should be designed around the security and privacy 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. [57]. 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. The device looked at contained multiple motion sensors as well as a light and temperature sensor, enabling for the capture of potentially exploitable data, such as the user's location/routine. This concerning attack is made worse by the fact that similar processors to the one attacked in this paper are used in similar pet tech devices. Given the rapid growth of the pet tech market, it is likely these processors would have been implemented in later devices, possibly put the users of them at risk of attack.

Mozilla's '*Privacy Not Included' [71] project provides consumers with a security and privacy guide for smart products. The purpose of this work is to help inform and protect consumers who may be looking to purchase or use newly developing technologies such as smart watches, consoles, and apps. Within this project, they look at several smart pet technologies including activity monitors, GPS trackers, cameras, and automatic feeders. The project provides consumers with the data collected by these devices and whether they meet a set of security standards, helping to protect potential users of these systems. Through providing expert reviews as well as the opinions of other consumers, this project shows the benefits of providing users with more information, allowing them to be better protected and confident in any smart devices they use.

As seen by the above sections, research specifically focusing on the security and privacy of these animal technologies is fairly limited. The current works largely focus on privacy or providing general security discussions, with the exception of one specific attack on a discontinued product. No work has been done to cover the apps relating to these products and any data that they may leak. Further user insights around security are also lacking, with the current studies just focusing on privacy. Given the limited focus on security, there are also limited mitigation/protection methods suggested in the current literature. The current studies mostly just suggest that the data collected by these devices should be treated with care, similar to non-pet-based products.

2.3 IoT Security and Privacy

Given the lack of research surrounding the security and privacy of animal technologies, especially security, we have also reviewed the literature on more general IoT security and privacy, looking at the methods and findings in research focused on similar technologies. This should give some context into how these other applications of IoT fair in terms of security and privacy and how animal technologies perform in comparison to them. This work also covers the identified challenges, security analyses performed on IoT, and user concerns to give an overview of how secure and privacy preserving these devices typically are.

The authors of [24], D'Mello et al., discuss the current practices and implications that arise through the use of IoT devices. This work also reviews the different types of security issues that need addressing for wearable IoT devices, including unautho-

rised access, attacking availability, and false data injection. Additionally, the paper highlights the regulations surrounding wearable devices. They found these regulations to be insufficient in many places where they typically only offered guidelines, with no enforcement. The authors also discuss challenges regarding data privacy, with promising improvements to secure data and user behaviour analytics via machine learning. This work gives an overview of the possible issue surrounding these technologies, both in terms of their vulnerability to a range of attacks, as well as ways in which the privacy of the users may be compromised.

Looking at the wearable technologies used by humans, instead of on animals, Ching et al. use the examples of Google Glass and smartwatches to show that real vulnerabilities have been present in these technologies [16]. The authors discuss the challenges and possible reasons for this, such as their limited processing power and bandwidth, and the unique new attack surface they bring. The authors also mention how comfortable the public are with these devices and how they feel these devices threaten their privacy. The challenges listed are not too dissimilar from those discussed around agritech devices [7], including power consumption and communication capacity, showing common themes across different applications. The lack of authentication by these devices and the challenges surrounding this are also discussed, mentioning the lack of an interface and the low processing power. This work highlights vulnerabilities that have affected real world IoT devices and makes clear issues hindering the implementation of effective protection methods, such as authentication.

One paper by Valente et al. [127], tests attacks on a variety of different IoT systems with different architectures. The authors show vulnerabilities in a range of IoT architectures used by real world systems, allowing for novel attacks against the devices that may be used in people's homes. These include attacks on children's toys and intimate devices, where an attacker was shown to be able to impersonate the children's toy or a trusted partner with control of the intimate device. The authors disclosed these vulnerabilities with the companies responsible, encountering mixed levels of responsiveness from them. Although these attacks are designed for human technologies, similar methods may be applied to technologies or wearables used with animals as well. This helps to provide insight into possible attack avenues for research, as well as clearly showing areas in which real world IoT devices are vulnerable to attack (showing where mitigation research may be necessary) and the impact an attack may have on the user.

More detail on the above mentioned intimate device attack by Wynn et al. can be seen in [137]. In this paper, the authors show the extremely concerning possibility

of privacy breaches and sexual assault via the studied intimate devices. This work shows that higher security and privacy standards are needed by those IoT devices that collect sensitive data and, in doing so, may put the user at risk.

Looking at the information exposed via consumer IoT devices, Ren et al. performed a multidimensional analysis on 81 devices [115]. They researched the destination of the traffic of these devices, as well as, the extent of the encryption, the data, and the content. They compare the regional differences between their UK and US studies, finding that in the UK, a greater number of devices were contacting destinations outside of the country. Furthermore, they found that the devices were exposing information to eavesdroppers, with a passive eavesdropper being able to infer user and device behaviour from the traffic of 30 out of the 81 devices studied [115].

A study [25] by Emami-Naeni et al. focuses on investigating user concerns related to Internet of Things (IoT) devices. This extensive study involved a participant pool of over 1000 individuals who were asked to express their privacy preferences within various provided scenarios. The findings indicate that "privacy preferences are diverse and context-dependent". Participants displayed a greater level of comfort with data collection occurring in public settings rather than private ones, and they expressed more comfort when data collection was perceived as beneficial to them. Additionally, participants expressed a desire to be informed about any data collection activities they were less comfortable with. The study also discovered that individual preferences could be predicted with a high degree of accuracy, up to 86%, by examining decisions made in only three data-collection scenarios.

In a study by Prasad et al., the authors delve into user concerns surrounding smart devices [81]. This particular paper concentrates on the worries expressed by parents regarding their children's utilization of smart devices within the household, such as the sharing of sensitive information, and the subsequent measures they employ to address these concerns, e.g., monitoring and controlling their use. The study also examines the potential benefits of these devices within the family setting. The authors gathered insights through a combination of focus groups and semi-structured interviews. The findings indicate that the use of these devices "may help build familial relationships and foster open communication". Furthermore, the paper highlights that parents feel a personal responsibility to shield their children from the threats posed by these devices, primarily due to a lack of trust in their inherent safety measures.

Focusing on IoT in smart healthcare, Karunaranthe et al. examine the current state of security and privacy of these Internet of Things devices used within the healthcare system [49]. This work covers the challenges encountered in implement-

ing security frameworks such as the limited power and processing capabilities, the increased priority, for reliability, interoperability, and durability. The authors call for the effective protection of sensitive and personal data suggesting the use of encryption and secure channels, highlighting the current lack of strategy in place for information gathering with these types of sensors. This work covers an important area, given that the majority of security breaches and data privacy issues are within the medical sector [49].

In an effort to work towards solving the complex security and privacy issues of physical IoT devices, Yao et al. divide up the life cycle of these devices [138]. They put forward an architecture for analysing the security and privacy requirements of IoT devices, dividing the system into post, in, and pre-working stages. Using this, they survey and sort the existing proposed technological solutions surrounding IoT security and privacy. They then discuss the present challenges, including the increased attack surface introduced by these devices (such as physical access), the balance between service and security and privacy, and the issues with static key management schemes in IoT environments.

Obaidat et al. provide an overview of IoT and its related security research, covering the applications, security architecture frameworks, recent security and privacy issues, as well as recent IoT security and privacy studies [76]. This work breaks up these attacks based on the three-layer architecture model (perception, network, and application) present in IoT networks. This work additionally gives detail on how attacks may target the CIA objectives (confidentiality, integrity, and availability), making clear how the users and operators of these systems would be affected. Examples of real world attacks on a variety of IoT applications is covered, such as those on smart cars and medical devices, highlighting what they refer to as the Internet of Vulnerabilities. Mitigation methods, countermeasures, and open research areas are additionally discussed, providing an overview of the current and potential future state of IoT ecosystems. Examples for possible key distribution and encryption methods, network protections, digital signatures are given, as well as discussing the additional resource-constraint-based trade-offs present in IoT devices.

These studies show that a range of security and privacy vulnerabilities continue to be found within real world IoT devices and systems. Studies of these technologies discuss the complex additional vulnerabilities and risks inherently present within these systems, such as the increased attack surface and reliance on resource constrained devices. These vulnerabilities necessitate the development of novel solutions that

take into account the identified drawbacks present in IoT devices, including animal technologies. Various studies also look into the user aspects of security and privacy with IoT devices, finding some discomfort with data collection within private environments. In our third study, we look to see how these users' perceptions and concerns translate over to the world of pet technologies.

2.4 Smart Building Security and Privacy

Due to the very limited amount of research into the user aspects of the security and privacy of pet technologies, we look into and provide an overview of user-focused research in smart buildings, where similar IoT devices are being implemented within people's living environments. Many pet tech devices are indeed being used in home environments and can be managed by similar smart home apps. While farm animal-based devices can be implemented within or alongside smart building systems.

The security and privacy issues of smart homes is a well-studied area. Given the increased use of smart devices within home environments, there is likely an increase in security and privacy risks. This is due to the introduction of more "vulnerable and unreliable devices" [141], 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, located up to half a meter away, via a side channel attack [140].

Other studies such as [15, 141, 121, 1, 25, 81, 142, 39, 46, 45, 122] have focused on the users' awareness and concerns regarding the security and privacy of smart homes and buildings and the IoT devices within them.

Chhetri at al. focused on examining user concerns related to smart home devices by analysing 128 online reviews specifically addressing smart home hubs [15]. Drawing from their findings, the researchers offer valuable insights aimed at enhancing the design of smart home devices, with the objective of mitigating these concerns.

The primary focus of a study by Zeng at al. revolves around addressing the privacy concerns experienced by individuals residing in smart homes [141]. To uncover these concerns, the authors conducted semi-structured interviews with smart home residents. The research revealed that many participants exhibited a limited technological understanding of smart homes, resulting in a lack of awareness regarding potential threats. Furthermore, even when participants were aware of certain risks, their overall level of concern was relatively low due to this knowledge gap.

In a similar vein, in a study by Tabussum at al., the authors carried out user studies using semi-structured interviews to assess the level of user knowledge and its impact on their perception of risks [121]. The study reveals that users' familiarity with their smart homes does not significantly influence their threat models. Instead, the research highlights that users' concerns are primarily shaped by their previous experiences with the companies responsible for designing these products in different contexts.

Abdi at al. narrow their focus to examine "Smart Home Personal Assistants", specifically exploring the users' perceptions regarding security and privacy [1]. To gain insights into these perceptions, the authors conducted semi-structured interviews. The findings reveal that users possess incomplete threat models, indicating a lack of comprehensive awareness regarding potential threats associated with their devices. This knowledge gap is attributed to incomplete mental models of these devices, leading to misconceptions about data storage and its subsequent utilization.

In the study conducted by Zheng et al., [142], the researchers employed semi-structured interviews with 11 individuals who were experienced smart home users. The objective was to gain valuable insights into their long-term experiences living with Internet of Things (IoT) devices. The findings revealed that users expressed "the need for improved privacy notifications and user-friendly settings". Additionally, the study highlighted that these smart home users exhibited a level of trust in IoT device manufacturers when it came to protecting their privacy.

Similar findings were found in a study conducted by Guhr et al. where the focus was on understanding how concerns regarding user privacy impact their intended usage of smart homes [39]. The researchers utilized an anonymous self-reported survey to gather data. The participants suggested the incorporation of more user-friendly interfaces to address privacy concerns effectively.

Badii et al. present Snap4City, an IoT platform capable of being deployed both on the cloud or on premise, designed to support smart city applications while adhering to GDPR privacy and security regulations [8]. The system offers more advanced security features compared to other IoT frameworks, with the authors performing a range of penetration and stress tests to ensure its robustness. Its architecture supports a wide range of IoT applications, from smart homes to large urban deployments, providing secure and efficient data management and processing. The system was piloted in cities such as Antwerp, Helsinki, and the entire Tuscany region, where it handled over 1 million of data points daily, demonstrating its effectiveness in a real world scenario. This platform demonstrates that solutions, even for large-scale scenarios such

Paper	Year	No. of Apps	App Type	Tools	Trackers	Traffic Analysis	Legislation Review	Privacy Notice Assessment
[128]	2016	1732	General	Lumen	✓			
[82]	2018	14,599	General	Lumen	✓			
[62]	2020	116*	General	Brave, Lumen	✓			✓
[63]	2021	30	FemTech	Lumen, Exodus	✓		✓	✓
[72]	2015	998,286	Web apps	apktool, Soot		✓		
[5]	2018	25	Health	Wireshark, SSL Labs, Fiddler		✓	✓	
This Project (Chapter 3)	-	40	Animal apps	Exodus, Lumen PI, Prolific	✓	✓	✓	✓

Table 2.2: Overview of previous mobile and app security and privacy studies. * - studied the corresponding websites, as well as the apps. PI stands for Privacy International's data interception environment [44].

as a smart city, exist for ensuring the secure and privacy protecting communications between IoT devices within a system/platform.

These studies find a lack of awareness of the potential risks caused by the use of IoT within these environments, potentially due to incomplete threat models. However, they do find that the level of knowledge of these topics does not necessarily influence their threat models and concerns. Our work will look to identify any similar lacking awareness or concerns with those using animal tech, helping to further realise the reasons for these attitudes towards IoT systems.

2.5 Mobile and App Security and Privacy Studies

The security and privacy of mobile apps is a well-studied area for more general apps, with a range of studies looking at possible attacks and information exposure, as well as those focusing on how well apps respect the user's privacy and adhere to the GDPR. We cover these works to reflect on the state of the more general app ecosystem, identifying possible tools and directions of study. We also look to compare the results and findings of these studies with those of our own, giving context to the security and privacy performance of animal apps. This allows us to see whether animal-based apps perform similarly to the overall app base, as well as other specific areas of apps, or whether they present issues unique to animal technologies. Here we provide details on these app security and privacy studies.

Focusing on the privacy of mobile apps, Vallina-Rodriguez et al. use the Lumen privacy monitor tool to present insights into the mobile advertising and tracking ecosystem [128]. The aim of this study was to identify and characterise the domains associated with mobile advertising, finding 58 that had not yet been reported by well-

known tracking and advertising domain lists. The Lumen privacy monitor is able to capture and analyse network traffic locally on the device by leveraging Android's VPN permission. This study of 690 users and 1732 apps, found that 60% of these connected to at least one domain, with users of news and social media apps being exposed to the most, given the web trackers embedded in the content [128]. The Lumen tool identifies the trackers that an app has contacted whilst the user is interacting with the app, allowing you to see what interactions may lead to these services being contacted and whether they are contacted before user interaction.

In a follow-up to this study, again using Lumen, Razaghpanah et al. identify 233 advertising/tracking services that were previously unknown to other blacklists and that the average mobile app connects to 11 different domains, with 75% of the 14,599 studied apps connecting to at least one advertising or tracking service [82]. This study involved 11,384 users from over 100 different countries, greatly expanding on the previous work.

In the study of the tracking behaviours, privacy notice presentation, user control options, and further privacy enhancing technologies present in top 116 EU websites and their apps, Mehrnezhad uses Lumen, along with additional tools [62]. They find inconsistencies in the ways in which privacy consent banners are displayed to the user in websites, browsers, and mobile apps, with these notices also not complying with the GDPR. Concerningly, many of these websites/apps begin to track the user right away, before the user has a chance to consent or deny, again not compliant with the GDPR.

Looking again at app privacy notices and tracking practices, Mehrnezhad et al. focus this time on fertility technologies, also addressing the differential vulnerabilities present in those using these technologies [63]. Using Lumen, as well as Exodus privacy, this work focuses on devices which collect very sensitive information that may be used against the user and even study the GDPR for mentions of this fertility data, with this not being mentioned directly. This analysis of 30 fertility apps finds that the privacy of the user is not respected through the appropriate measures, given the sensitivity of this 'special category' data being handled.

Focusing more towards the security of mobile apps, a study by Mutchler et al. on 998,286 mobile web apps (all available free web apps as of June 2014), found that 28% of the apps studied had at least one vulnerability [72]. When analysing for trends, they found these vulnerabilities across the app ecosystem, being present in top apps as well as libraries. The study looked for the presence of unsafe navigation, content retrieval, certificate validation, leaky URLs, exposed POST requests, expired

Paper	Year	Purpose	Sensors Used	Motion Type
[134]	2015	Fingerprinting/Authentication	Touch,Accelerometer,Gyroscope	Hand Gestures
[66]	2015	NFC Payment Verification	Accelerometer	Tapping
[75]	2018	Smartwatch 2FA	Pressure,Size of touch	Tap screen to melody
[55]	2015	Fingerprinting/Continuous Authentication	Accelerometer,Gyroscope,Magnetometer	Holding/walking
[40]	2018	Artificial Ambient Environment for data transactions	Accelerometer,Gyroscope,Gravity,Linear Acceleration,Magnetic Field, Rotation‡	Vibrations
[61]	2009	Secure pairing of mobile devices	Accelerometer	Shaking
This Project (Chapter 4)	-	Authentication	Accelerometer	Physical tapping devices together

Table 2.3: Overview of previous motion-based authentication studies. ‡ - one sensor used at a time (decided when ran).

domains, and library vulnerabilities.

The study by Aliasgari et al. focuses on the top 25 health apps, analysing them for security and privacy vulnerabilities. They examined the apps' use of TLS and ran an MITM attack to see what data is collected and transmitted to servers [5]. The results of this study are very concerning with 12 of the apps revealing passwords when attacked. Additionally, of those 12 apps that collect and transmit protected health information, only 1 passed the TLS configuration test. These tests were done on Android 6.0 using WireShark, SSL Labs, and Fiddler for the analysis.

A slightly older study on mobile health app S&P, providing more of a review and recommendations was done by Martínez-Pérez et al. [60]. This work gives an overview of the current literature at the time (2015) as well as the existing laws regarding security and privacy in mobile health apps. The recommendations they provide are aimed towards those designing these apps, with suggestions towards topics such as access control, authentication, data transfer, and retention, as well as informing the patients before collection and after a breach. Specific technical methods are mentioned in these recommendations, such as recommended key sizes, providing a solid basis for future recommendations for similar app sets.

Little research has been done into the security and privacy of apps when they are designed for use with pets and livestock. This could be due to an even lower concern regarding the privacy of apps used with animals compared to other apps, as found in [129]. Our first study within this work aims to cover this research gap and see if animal technology users' security and privacy is at risk.

2.6 Sensor-based Authentication

Looking towards proposing a possible improvement to one aspect of IoT security, we research IoT authentication and the possibility of an easy to implement solution. Given the lack of an interface and the lower power capabilities on many IoT devices, including animal tech, authentication can be a challenge. Here we review a selection of the literature surrounding the current problem-space of IoT authentication selection of the literature surrounding . We also cover works highlighting the possible alternative methods for authentication, utilising the available sensors typically already present within these devices. Here we look to build upon those works focused on motion sensors, e.g. accelerometers, which are common with animal devices (as well as many other IoT devices) and simple to interact with.

The work performed by Fomichev et al. [32], provides both a survey of secure device pairing methods, as well as a model for effectively comparing them. They find that data confidentiality of the physical medium being used is hard to guarantee in practice, leaving these systems vulnerable. They highlight the importance of building pairing schemes that are resilient to user misbehaviour, observation of the user actions during the pairing process, and honest-but-curious adversaries. The authors summarise the physical channels used, as well as the HCI channel, evaluating the methods in terms of usability, security, and the current pairing schemes that use these. The paper emphasizes the need to shift to a use-case-oriented design to ensure the security and effectiveness of these pairing systems.

Looking at the general feasibility of utilising on-device sensors for mobile phone authentication, Wang et al., focus on the fact that users perform gestures in different ways [134]. They capture two aspects of these gestures: the geometry and timing of the user's hand; and the displacement and rotation of the devices (using the accelerometer and gyroscope). They are able to fingerprint users based on this collected data, achieving less than 2.5% false accept and false reject rates. Importantly, even when an attacker is able to directly observe the gesture collection process, they are only able to successfully bypass the authentication process 3% of the time.

In the work by Mehrnezhad et al., they look to use the action of tapping as a means to prevent mafia attacks against NFC payment machines [66]. They suggest the use of tapping a device against the reader to generate a shared unique key between the user's device and the reader. This paper then uses this shared information to verify the payee and ensure that an attacker isn't relaying the payment data to pay for some other item. This solution was found to work even when the attacker is in a

nearby location or a similar environment, unlike the other previous ambient-sensor-based solutions. The implementation of this solution would also be very cheap and allow for backward compatibility. This form of a shared key may also be applicable to animal tech, where many of the devices are already equipped with motion sensors for their regular functionality.

The proposed authentication method TapMeIn also looks to use the idea of tapping against a device to aid in the authentication process, by allowing it to recognise a specific user [75]. Here, Nguyen et al., use the user's tapping of a smartwatch device to a melody to authenticate that it is the correct user. The system is trained off of the actual user and is able to distinguish them from an attacker attempting to impersonate them, with an accuracy of 98.7%.

In previous work, also looking to identify specific users using the sensors available on a device, Lee et al., use a mixture of motion-based sensors [55]. They focus on the accelerometer, orientation sensor, and magnetometer present with smartphones, training a system to recognise a specific user. They find that the authentication accuracy for the orientation sensor degrades more over time and that the accelerometer and magnetometer sensors are more stable. They are able to obtain promising results obtaining an accuracy of 97.4% when utilising all sensors, on one of their datasets.

Looking again at the use of motion sensors, Gurulian et al., focus on the utilisation of vibrations caused by one or both devices [40]. This data is used in an attempt to prevent relay attacks using the detected vibrations as an artificial ambient environment (AAE). The proposed system compares the patterns detected within the two devices, looking to see whether similar motion data was been detected. They find that their solution performs better than previously proposed Proximity and Relay Attack Detection (PRAD) mechanisms, able to achieve an EER of 0.001 using the gyroscope data and certain machine learning classifiers.

Experimenting with a shaking method, Mayrhofer et al. propose a method for authenticating mobile phones without the need for a third party to be introduced [61]. This shared knowledge generation involves the user holding both devices in a hand and shaking them, with this shared motion data being used for authentication. The authors test multiple algorithms, finding a system based around comparing the coherence of the tapping signals to be the most effective. They are able to achieve an FAR of 0% and an FRR of around 10%.

Looking at the usability and real-world applicability of tapping-based authentication methods, Marques et al., perform a user study, seeing whether the same level of security and usability standards can be met with these methods [59]. In this work,

the participants are tapping a phone screen, with the time between these 'on' and 'off' aspects of pressing the screen being used to derive the pattern used for authentication. Compared to PIN and draw unlock, they find the usability and resilience to shoulder-surfing comparable. The study finds that this sort of tapping method could also be appropriate for situations where the user is wanting to unlock their device inconspicuously. This is potentially due to the perceived increased difficulty in performing a memorised tapping sequence.

The above works show that there is promise within the utilisation of motion sensors, such as accelerometers and gyroscopes, as part of some form of authentication procedure. Tapping and motion-based methods have shown to be effective within similar scenarios on similar types of systems (mobile). Our work within our second study will look to build on these works and identify whether there is potential for this sort of authentication method for IoT devices.

Chapter 3

Security and Privacy of Animal Apps

This chapter presents the process and results of our system studies i.e. security and privacy assessment of popular animal Android apps.

3.1 Chapter Introduction

Given the growth of technologies in use for both farm animals and pets, phone-based apps are also becoming increasingly common. These apps typically allow for the user to view and interact with the data collected, with some apps also offering social elements. These apps will collect/contain a range of information about both the animals and those humans interacting with the animals and/or the apps.

Despite all of this data being collected, the security and privacy features of these technologies have been found to be lacking in various ways, with no information on whether the corresponding apps operate securely. This lack of focus on their security and privacy may be due to the current complete lack of regulations on animal data, as well as the lack of regulations surrounding the agricultural technology (agritech) field. Through an analysis of top-ranking animal welfare legislation, we find no explicit mention of these smart technologies and no mention of the security and privacy of animal data and the owner. Similarly, the GDPR is also lacking in these areas and does not apply to data from which you can identify an animal [83]. This is regardless of the fact that these systems collect information about their human users too [132].

As the demand for animal technologies increases by end-users, for both farm [12] and companion animals [104], these industries offer more solutions that are potentially not secure. This is especially concerning for the farming sector, a critical national

infrastructure in any country [4], that will likely be the focus of future attacks. Despite the smaller scale of attacks on companion animal technologies, their lack of security and privacy considerations are also concerning. Pet theft has reportedly increased over the past year, which can have an undeniable emotional impact on their owner [111] and may put people with special needs who have an animal aid at risk. Hence, a comprehensive research is required to assess and analyse the current security and privacy practices of technologies present in these industries. Table 1.2 shows examples of possible cyber-attacks on these systems which can potentially affect the animal, owner, farm, and wider society.

The research in this area is sparse and only a few previous works have addressed the security and privacy issues of animal technologies [9, 132]. In this chapter, we evaluate the security and privacy features and practices of popular farm and companion animal Android apps. First, we perform a review of the existing animal welfare legislation, as well as the more general data protection laws, looking for mentions of animal technologies and potential privacy and security issues. Second, we build a data set of 40 popular farm and companion animal Android apps for our evaluations. We make this list publicly available for other researchers to conduct further studies. Third, we perform our experiments using a wide range of security and privacy evaluation methods and tools including static, dynamic and network traffic analysis, as well as privacy notices and tracking evaluation according to data protection laws.

Our findings highlight that serious security and privacy vulnerabilities exist in these apps. Several of the applications in our set exposed user login information in their non-secure HTTP traffic. In addition, many of the apps sent information to tracking services before the user is able to consent and made little effort to effectively gain consent from the user regarding their privacy policy.

We also have communicated the serious security vulnerabilities (i.e., sending username and password in plain text) to the app companies and contributed towards fixing their products. To date, two companies replied to these concerns (PoochPlay and FarmWizard) and stated that they will look into the issues behind this vulnerability. Accordingly, they worked on updating their apps. After testing a few months later, these two apps were found to no longer present this vulnerability, no longer putting user's at risk of attack. The app belonging to the company that did not respond still presented the vulnerability during this retesting.

The work in this chapter serves to give an initial indication of the state of security and privacy in animal technologies. Our results help to inform future work, including our own, showing that poor practices are present that may be putting real world

users at risk. This indicates that more thought needs to be put into designing these technologies in a way that makes them secure and respecting of their user's privacy.

3.2 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 security and privacy, in animal-based legislation.

3.2.1 Approach

We selected the top-ranking animal welfare legislation, as ranked by [114] and [94], for our analysis. The animal welfare legislation that we look at include those from Austria [97], Denmark [86], Germany [92], the Netherlands [98], Sweden [109], Switzerland [91], England and Wales [110], and the OIE (World Organisation for Animal Health) [112]. We also look at the General Data Protection Regulation (GDPR) [29] and California Consumer Privacy Act (CCPA) [106], along with its recent amendments [107] 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. On top of this, we 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 but with animal-focused words (such as farm, pet, and wearable) and a review was done of the sections like before. We believe that this review of the legislation effectively highlighted any mention of data collection and animal technologies within the animal welfare legislation. Our selected keywords covered any effective mention of these animal technologies within the legislation, finding data-related, but otherwise unrelated discussions. Similarly, our animal-based keywords for the GDPR and CCPA covered the terms necessary for even a basic discussion on animal-related data collection.

In addition to directly reviewing a selection of legislation, we also discussed this area with experts in animal tech in academia and industry (including farmers). They confirmed a lack of dedicated security and privacy policies in these industries with security and privacy not being considered by those designing and using these technologies.

3.2.2 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 [83]. Furthermore, there is no mention of animal applications, smart technologies, or the data that they collect in the current animal legislation in the UK [84, 85], or the codes of practice for pet owners [88, 87] despite the growing use of these technologies. Similar to the GDPR, the CCPA has no mention of these animal-related technologies and is focused solely on the privacy of human data within systems.

A further review of the top-ranking animal welfare legislations also finds details of these technologies to be lacking. Within them, there is no mention of the use of smart technologies, with the closest being that new technologies can be tested on animals [109], the mention of RFID in ear tags, and that electronic devices used in facilities should be safe for cattle [112]. In terms of the data collected about animals, the Swiss legislation states that animal data includes the data from monitoring animals and "the results thereof" [91]. In Austria, pet-related data is removed after a fixed period, 20 and 25 years for dogs and cats respectively [97]. However, this is not for privacy reasons and is just to clear their system of any undeclared dead pets. The OIE mention the recording of production data for an animal health management system [112], however, this is vague and there is no mention of online or smart systems.

This lack of legislation is not due to a lack of care towards animals, with these legislations recognising the need to protect animals with special laws. Austria believes that "the welfare of animals should be held to a value equal to humankind" [51] and the UK government is implementing a pet theft task force, along with longer prison sentences, to help prevent the "undeniable emotional impact" of having a pet stolen [111].

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 all of 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.

Through reviewing the legislation, we had hoped to see mentions of animal-based data. Given the growth of this area, we expected to see these technologies being mentioned within Animal Welfare legislation, with at least some reference to the data collected. Ideally, precautions around maintaining the security, privacy, and integrity of such data should be provided, particularly around those systems used in agritech.

Regulations such as the GDPR and CCPA should look to cover those devices that may more so indirectly collect human-related data, such as animal technologies and other emerging areas of IoT.

3.3 Methodology

In this section, we explain how we prepared our app set, as well as our security and privacy evaluation methods and tools. We have conducted our experiments between Mar to Jul 2021 in the UK which is currently complying with the GDPR.

3.3.1 App Set

An equal number of pet and farming-related applications were selected for analysis (20 each). We believe that this selection of apps allows for a good overall view of popular animal-related apps. Here we describe our selection process for both the pet and farm applications:

Pet Apps: Where possible, apps were selected from the device set used in [132]. 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, 15 in Table 3.1). For the remaining apps, the most popular pet device applications, that were also functional, were selected. These apps are 2, 5-7, 9, 13, 16 in Table 3.1. 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 again chosen based on their popularity (the most downloaded), but also with the ability to either create or login to an account (17-20 in Table 3.1).

Farm Apps: Again, where possible, the farming apps were chosen from the device list in [120]. This paper reviews the validated and commercially available sensor technologies that may be used on dairy cattle. From this paper, 15 apps were found that are available on the Google Play Store, functional, and with account creation or login available. These apps are 21, 27-40 in Table 3.1. For the remaining 5 farming applications, the most downloaded apps where account creation or login is possible were selected (22-26 in Table 3.1).

3.3.2 GDPR Requirements

In order 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

system. This includes informing the user what these tracking services do and why they are being used. They must also get the user's consent to use this tracking data collected about them. The ICO [101] 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/visit the web service. To gain this consent, the user must perform an unambiguous positive action, e.g., ticking a box or clicking a link. This action of confirming consent should also be not be linked to other matters such as the terms and conditions; the user should be solely giving their consent to these tracking technologies. Whilst gaining consent, the providers must also avoid the use of 'nudge behaviour' that may affect the user's choice. This gaining of consent must allow for the user to make a choice, and so must include options to both accept and reject.

It is also not a valid form of collecting consent if the user is blocked from accessing the service's content unless they accept. This would involve a privacy notice that only gives the user the option to accept, appearing prior to access to the content, preventing the user from interacting with the service unless they accept. This is not valid as it will nudge users to agree to a privacy policy that they may not agree with, just so they can access the service. Another form of nudging would be to highlight the Accept option over the others such as Reject, etc.

Users should be able to take back their consent that they have previously given as easily as they were able to give it. Providers should also not rely on other outside mechanisms to determine the user's privacy control preferences, such as browser or mobile settings. Having the tracking technologies enabled before the user is able to explicitly give their consent via a positive action is a violation as consent has not been correctly obtained.

3.3.3 Methods

We use various methods to evaluate the security and privacy of our set of apps (Table 3.1).

Static Analysis: a method of analysing software that involves examining the code, but without executing it. This is typically done to find errors with a program's code before it is run. However, static analysis can also be performed to identify certain names or features within a program's code. Android Lint[1] and SpotBugs [2] are examples of static analysis tools that can be used to analyse programs for errors.

[1] developer.android.com/studio/write/lint
[2] spotbugs.github.io

Parasoft [3] is another tool, that can be used to enforce privacy regulations by testing rules on the code. The static analysis tool used in this paper is Exodus Privacy[4], which is explicitly designed for identifying trackers and what permissions are used for apps and has been previously used in [63].

Dynamic Analysis: involves testing or evaluating the program whilst it is running. When designing software, dynamic analysis is typically used to test the performance of the program. Similar to static analysis, dynamic analysis tools are usually designed for this reason. Tools such as eclipse [5] can be used to test the performance of programs step by step while they are running. Hooker is another tool that is used to "intercept and modify any api calls made by the targeted application" [6]. The tool Lumen Privacy Monitor [7] 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 [128, 82, 62, 63].

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. Network Traffic Analysis is typically achieved by intercepting the network traffic from the program, before passing it back on to its destination, like in a man-in-the-middle attack.

One of the tools for this method of analysis includes Android tcpdump, which captures packets from any "network connections you may have on your Android device" [8]. Whilst useful for capturing the packets, tcpdump does not allow the user to view encrypted traffic. Another existing system is SandDroid, which can capture "network data during an APK's running period" [135]. Sanddroid can be used to look at the HTTP traffic sent through an Android device, as well as any SMS messages. However, like tcpdump, Sandroid cannot be used to view encrypted traffic.

The two tools used in this paper are Lumen Privacy Monitor and Privacy International's data interception environment[9]. They were chosen as they are able to decrypt the packets from HTTPS traffic, allowing them to obtain more information about the network activity of the selected applications. These two tools have been specifically designed for the analysis of application privacy, making them ideal to use

[3] parasoft.com
[4] exodus-privacy.eu.org/en/
[5] eclipse.org/ide/
[6] github.com/AndroidHooker/hooker
[7] haystack.mobi/
[8] androidtcpdump.com/
[9] privacyinternational.org/node/2732

in this paper. Privacy International's data interception environment was designed for [103], which highlights its effectiveness at monitoring an app's network activity.

Privacy notice analysis: In order to analyse the privacy policies of the selected applications they were opened on a prepared Android device. Where account creation was only possible online, their corresponding websites were opened on Google Chrome. In each of the apps, we observe how the privacy policy is presented to the user if it is even presented at all.

We look for if 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 app, their websites were looked at to see whether the privacy policy was clearly displayed to the user. This did not include the privacy policies of some companies, which are just linked to at the bottom of their websites. Similar privacy policy studies have been conducted in [62, 63].

Note that some of the systems looked at required access either to the physical devices they link to or an actual farm. If it was not possible for us to create an account we looked at how the privacy policy was displayed on their website and if it was mentioned when requesting a demo. This limited our ability to fully observe the privacy policy practices of some of the app set.

3.3.4 Tools

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

Android Device We perform our experiments on an Android device (Google Pixel 3a) where we study the permissions requested, tracking services communicated with, as well as the security of the communications made by the mobile apps. As standard for this area of research, we focus solely on the Android ecosystem due to the more secure restrictions present in iOS devices that make these types of system studies more difficult. Similar studies may be possible in the future, looking at the 'protected resources' (iOS equivalent of requested permissions) requested by the iOS versions of the apps, alongside the trackers and security. Those studies that have been performed on iOS app privacy have found that they perform similarly to Android apps [53], despite the differing set of development privacy practices within these ecosystems [37].

Exodus Privacy: Exodus Privacy is an online system that analyses Android applications, looking for embedded trackers. It does this by performing a "static

analysis of APKs and compares the Java class names with a list of known trackers" [90]. This tool is incredibly easy to use and has a large number of already tested applications that can be checked, speeding up the analysis process.

Exodus produces reports listing the trackers and permissions, marking whether permissions are potentially dangerous. It is able to perform this due to the fact that applications running on JVM have class names that are readable directly in the binary file of the program and therefore do not require decompilation [89]. Exodus runs dexdump[10] 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 [89].

Lumen: Lumen is an Android app that uses dynamic analysis to perform a similar task to Exodus. However, 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. Lumen also performs network traffic analysis to aid in the analysis of the applications' communications. Lumen also supports TLS interception to help identify privacy leaks inflicted by apps, over encrypted traffic, in real-time [102]. This allows for the app to reveal the tracking services other apps are communicating with, as well as any device information they are leaking.

Due to changes in how Android handles trusted credentials, a Google Pixel 3a was reverted to Android 9, allowing for Lumen to install its own CA certificate. The selected applications were then ran without any further interaction, with Lumen active, and were left open for two hours. This would allow us to capture the trackers communicated with before the user is able to 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 3.1.

Privacy International: In order to find out whether pet and farming apps communicate securely, the Privacy International data interception environment was used. This environment allows the user to capture all of the communications made through an Android phone. As well as this, the environment 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.

[10] `android.googlesource.com/platform/art/+/master/dexdump/dexdump.cc`

Because of the previously mentioned changes to how Android handles trusted credentials, a Google pixel 3a was reverted to Android 9 and was also rooted, allowing for a CA certificate to be manually installed.

When using the data interception environment, all applications were closed, ensuring only the selected app would be active. mitmproxy [11] 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 into due to errors, such as Tractive and Sensehub, with other apps not allowing an account to be created due to a lack of the corresponding device or not owning a farm. After being left for 10 minutes, mitmproxy was stopped and the results were analysed using mitmweb.

3.3.5 Ethics

Ethical approval was obtained through Newcastle University before any of the research took place. Due to the involvement of animal-based information in some of the farm-based systems, the project was approved by the Animal Welfare Ethical Review Body of the University.

3.3.6 Limitations

As mentioned in section 3.3, an older version of Android had to be used to allow for both Lumen and Privacy International's data interception environment to be used. Running the apps on an older version of Android 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 UK Android devices in 2021 [108]. Our experiments took place in March, April, and July 2021, where the percentage of users, in the UK, for Android 9 and lower was around 40% [95]. Worldwide, it was more than 50% [96]. 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 also the possibility of Exodus giving false positives. This is due to the fact that static analysis tools may detect trackers and permissions in the app's code that are never actually used. However, even if not used, the presence of these trackers is still concerning as they may be used at a later date. We also use our Lumen analysis

[11] mitmproxy.org/

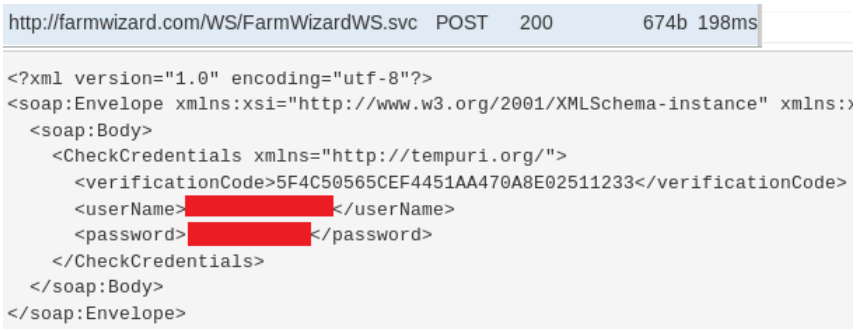

Figure 3.1: Example of a farming app revealing the user's login details.

to identify only the trackers communicated with during testing, before the user can consent. Hence, it may be the case that multiple other trackers become activated if a user engage with the app otherwise. Six of the apps (3, 19, 22, 31, 38, 40 in Table 3.1) did not appear in Lumen even after being opened with Lumen running. 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. This result is shown through an X in the Lumen Trackers, Permissions column in Table 3.1.

Whilst running Privacy International's data interception environment, 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 and can be seen as an example of good security practice. 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 actually mean they are more secure against a man-in-the-middle attack. Three of the applications (10, 14, 34 in Table 3.1) 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 six of the apps (3, 5, 15, 23, 30, 33 in Table 3.1) could be opened, however could not be logged in to whilst running the environment.

There were also fourteen applications that were unable to be logged in to even while the environment was not running. For two of these apps (21 & 22 in Table 3.1), this was due to issues with the application, potentially due to running the experiments on an older Android version. The other twelve applications (24, 25, 27, 28, 30, 31, 34-39 in Table 3.1) were unable to be logged into as they required an actual farm, or access to the related equipment, in order to set up an account. For these apps, a login attempt was still tested with incorrect login credentials, allowing for this

communication of login details to still be observed and analysed.

The security vulnerabilities identified through the use of Privacy International's data interception environment are only a subset of the possible vulnerabilities. Some of the applications may have been able to hide their poor security practices from this analysis, but may still be vulnerable to a more advanced attack. However, our analysis and findings are still vital as they highlight a clear and dangerous vulnerability that is putting the current users of these systems at risk.

3.4 Results

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

3.4.1 Security Vulnerabilities

A couple of different security vulnerabilities were found in three of the applications, using Privacy International's data interception environment.

Password in plain text

Three of the applications studied (FarmWizard, 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 one of these apps will be able to find out their login information. An example of this can be seen in Figure 3.1. Collectively, these apps have over seven thousand downloads, the users of which could be exposed to an attack due to this vulnerability.

For one of these applications, this vulnerability is especially concerning. Accounts on FarmWizard are shared between multiple users, with there being only a few accounts per farm. Alongside this, an individual user can change the account password once logged in, allowing for an attacker to deny access to this service for many users at a farm.

The other 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

Figure 3.2: User information displayed in plain text in the HTTP traffic of a Pet app. User details have been anonymised.

user information, such as their address and phone number, as well as the pet-related information that it collects. If a user has filled in this account information, then it is easily accessible to any attacker with access to their account.

User information in plain text

In addition to login information, two of these apps (PoochPlay and Pawtrack) also showed some 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 3.2 (bottom). Details about the user's pet were also visible, including whether the pet can swim, medical conditions, medicines they take, and their 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 3.2 (Top).

3.4.2 Privacy Vulnerabilities

As well as these security vulnerabilities, a few privacy vulnerabilities were also found.

Trackers

All but four of the applications were 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" [28]. An increased number of trackers will mean that either more data is being captured about the user or it is being distributed to more 3rd 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). Despite this, this group also features one of the few apps without any trackers detected by Exodus, Pawfit.

In terms of the Lumen results, 21 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 and farm-related apps (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), pet health (15.33), and farming apps (14.44) respectively.

On average, the farming apps have under half the number of trackers (1.95), found by Exodus, than the average of the other application types (4.1). However, they have slightly more permissions (14.55) than the pet health apps (14). This same permissions result can be seen in the Lumen results mentioned above.

Only five of the applications were found to have leaks from the Lumen analysis. Three of these applications also requested higher than the average number of permissions. Interestingly, three of these five apps were farming applications, which had a lower than the average number of trackers and permissions.

Collecting information about a user through trackers is fine, as long as the application first gets the user's consent. Applications that are sharing user data through trackers or leaks prior to getting consent from the user, via the privacy policy, are violating the GDPR.

Table 3.1: 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 3.5. Explanation of Privacy Policy symbols can be seen in Figure 3.3.

No.	App Name	App Type	no. Users	Exodus Trackers, Permissions	Lumen Trackers, Permissions	Lumen Leaks	Privacy 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
21	Sensehub	Farm	10k+	4, 12	0, 12		X
22	FarmWizard	Farm	1k+	0, 19	X		X
23	HerdWatch	Farm	10k+	4, 31	2, 31		X
24	BreedManager by Moocall	Farm	10k+	1, 12	0, 11	1	X
25	iLivestock	Farm	500+	1, 12	0, 12		✓
26	Stock Move Express	Farm	1k+	1, 8	0, 8		X
27	CowManager	Farm	10k+	4, 10	0, 10		X
28	BCS Cowdition	Farm	10k+	1, 6	1, 7		X
29	Boumatic	Farm	100+	1, 5	0, 5		✓
30	Digitanimal	Farm	5k+	1, 24	2, 14		-
31	SireMatch	Farm	1k+	0, 1	X		X
32	MooMonitor Plus	Farm	1k+	1, 11	0, 11		X
33	DeLaval MyFarm Beta	Farm	10k+	1, 8	1, 8	1	✓
34	Ida	Farm	500+	6, 25	4, 25	2	X
35	FarmView	Farm	5k+	4, 17	0, 17		-
36	Fullwood Packo M2erlinInfo	Farm	1k+	3, 8	0, 8		X
37	smaXtec	Farm	1k+	2, 28	1, 29		X
38	Sensolus	Farm	100+	0, 9	X		-
39	FarmLife	Farm	1k+	2, 27	1, 27		X
40	Lely T4C InHerd - Cow	Farm	10k+	2, 15	X		X

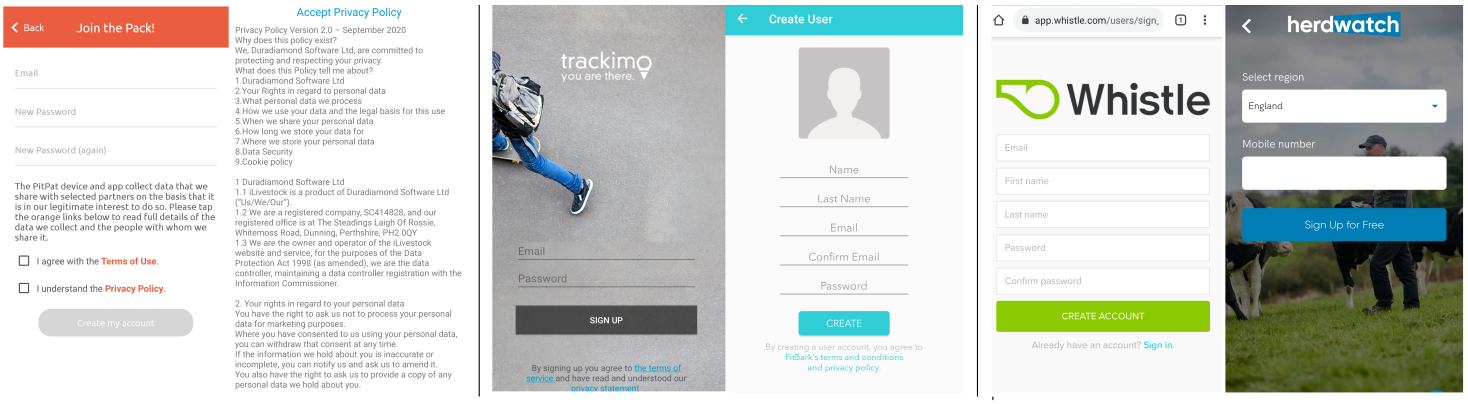

Figure 3.3: Account creation of 6 animal apps - Left(✓): PitPat and iLivestock; Middle(-): Trackimo and FitBark; Right(x): Whistle and HerdWatch. ✓means that the privacy policy is clearly displayed to the user and that they explicitly have to accept it. – means that although the privacy policy is mentioned, 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.

Privacy policy

Overall the apps perform very poorly in terms of notifying the user of their privacy policy. Whilst many of the apps do have a small message saying that you are agreeing to their privacy policy, only four of the apps get you to explicitly agree to this, as seen in Figure 3.3. These apps, 1, 25, 29, and 33 in Table 3.1, clearly display the privacy policy to the user. Thirteen of the remaining apps just provide a link to their privacy policy instead of displaying this to the user, like in the middle row of Figure 3.3. This goes against the requirements of the GDPR, which requires consent to be explicitly given by the users [136], something that is unlikely to happen with most of these apps. The majority (23) 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 in the bottom row of Figure 3.3.

Another concern is that 21 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 3.1. As stated in article 6 of the GDPR, the processing of user data can only be lawful if the data subject has given consent [29]. None of the apps give the user the ability 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" [136].

3.4.3 Communication with Industry and Re-testing

After discovering several security vulnerabilities that may put the user at risk, the companies (more specifically, three 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. 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 at least at three different occasions with one week time between each email; making sure that such an email does not get ignored.

Out of the three applications with these security vulnerabilities, two of the companies replied to our emails to date. Both of these companies (FarmWizard and 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 the serious security issues several months after communicating these issues to their respective providers. For this, we used the exact same methods as before, making sure that the applications were updated to their latest version. FarmWizard and PoochPlay, the two apps who we heard back from, no longer reveal any user details. PoochPlay now operates more securely, using https for all of its communications. FarmWizard still cannot be logged into, however, it does not reveal the login attempts, stopping before this can take place. PawTrack, on the other hand, still presents the same issue as before. The user's email and password are clearly visible in a http message. This lack of a fix is not surprising given that we did not hear back from its company.

3.5 Discussion

In this section, we discuss how regulations and industrial practices, as well as educating the end-users of these technologies, can address some of these security and privacy flaws in the future. We also compare our work with the previous work in different sectors.

3.5.1 Risks to Human Users

Given the focus these devices and systems have on animals, the data they collect is less likely to be viewed as personal or sensitive [129]. In the case of many pet technologies, including those in this study, this is not the case, as these applications also collect or store information about their user. However, with the focus not being on the human users, these systems may not be designed around the security and privacy needs of the human users. This could explain the lack of privacy policies and seeking of user consent in relation to privacy. Given that humans are the real users of these products, these apps should be designed with the security and privacy needs of people in mind.

With Industry 4.0 and the ever-increasing connectivity between devices, extra care should be given when handling personal data. The smart animal wearables that connect to a few of these apps, as well as the smart farming services are examples of these IoT technologies and should therefore be designed with increased security and privacy concerns. This increased connectivity is especially concerning given the increasing use of these technologies in both the farming and companion animal industries [12, 104].

On top of this, many of these applications collect personal data regarding the user and therefore should follow the GDPR and other privacy policies designed around humans. As shown in [132], many pet applications even collect more data about the human user than their pet.

An attacker with access to the data these devices capture, through exploiting an insecure authentication process, would potentially be able to track the human user, aiding with further crimes such as robbery, burglary, or pet theft. Access to just the account details would aid in the design of phishing attacks targeting these users and may allow an attacker to impersonate the user in the social sides of these apps. With the clear risks of an attack against their users, these apps must be designed securely and prevent user information from being revealed to a malicious party.

Another issue with these apps is the dual usage of such technologies. The GPS trackers that we looked at do not have to just be used on animals, with them potentially being used on people as well. There is nothing restricting these devices from being reused or specifically purchased to track something other than an animal. One of these devices even directly advertises its possible use on children, alongside pets and cars (Trackimo).

Authors of [129] found that people use these trackers on children, the elderly and the impaired. As most of these devices are not designed around using them on humans they likely will not be as secure or protect the users' privacy as well.

Given the possibility of consumers using these devices, not just on pets, they should be designed to the security and privacy standards that a human tracker or activity monitor would.

3.5.2 Comparison with Related Work

In this paper, we found that 35 (87.5%) of popular animal apps have at least one tracker and that 10 (25%) have at least five. This shows that our studied apps are more likely to have a tracker than those studied in [128] (60%) and [82] (75%), analyses of more general apps using Lumen. More of our studied apps have at least five trackers than [128] (20%) and our app set has slightly less than [82] (29%). Like in [103], we found apps communicating with trackers before user interaction could enable consent. However, this was only the case for 21 (52.5%) of our app set, compared to 61% of theirs communicating specifically with Facebook.

We found that our app set performed worse in terms of their privacy policy than those studied in [62], which looked at the top 116 EU websites and their corresponding apps and, [63], a study on popular Android apps for women's fertility management. In [62], they find that 51% of their apps have no privacy notice and [63] has 40%. In comparison, 57.5% of our apps did not display any privacy policy.

Our results show that 3 of the analysed applications have a serious security vulnerability that reveals the user's login details. Whilst a lower percentage than that of a much larger scale study of all available free web apps at the time, [72] (28% with at least one vulnerability), we were only looking for one type of security vulnerability. This percentage is also lower than what was found in [5], a study of 25 health apps designed for humans, where 48% of their studied apps revealed user login details via a man-in-the-middle attack. This study, however, was performed on an even older version of Android (6.0). Also, their attack is less serious as it requires decrypting the intercepted login messages. Whereas our results specifically highlight non-secure communications that do not need to be decrypted to see the user's login details during its authentication, a much more serious vulnerability.

On top of the security vulnerabilities identified in this paper, another 14 applications were observed to handle user data poorly from the Privacy International analysis. 12 of these applications (4, 7, 12, 16, 17, 18, 26, 27, 32, 35, 37, 38 in table 3.1) had the user's login details visible in https messages and the remaining 2 had images visible, the first being the user assigned dog picture (20 in table 3.1), and the second showing an image of the user's location (6 in table 3.1). While this is

secure against basic traffic interception and observation, it is bad practice and may still put the user in danger if the attacker is able to decrypt the messages as done in this paper.

Overall, the apps studied in this paper have worse privacy in terms of trackers than larger more general app sets [128, 82]. However, they perform better than apps in other studies with more condensed and concentrated app sets such as [103, 62, 63]. The two groups of apps looked at (pet and farm-based) generally perform very differently in terms of privacy, with farm-based applications having far fewer trackers on average. However, despite having fewer trackers than the apps from these studies, our app set performed worse in terms of displaying and getting consent for their privacy policy. Despite fewer of our studied apps having security vulnerabilities than those in [72, 5], our results are still extremely worrying with 3 of our studied apps having a dangerous vulnerability that could be very easily exploited to attack a user.

3.5.3 Industrial Practices and Regulations

As mentioned before, many of the applications looked at violate the GDPR in some way. This includes not giving the user the option to opt out of the privacy policies, as well as sending user information to tracking services before the user can consent to this. There are currently no regulations on animal data privacy, meaning this would not technically be an issue for the pet apps if they did not also collect data about the user.

Our review of various legislation has shown that the security and privacy of these animal-based systems have not been considered. There is no mention of these technologies within the top animal welfare legislation, the GDPR and the CCPA. This leaves those using these systems susceptible to poor practices that may leave them vulnerable to having their privacy exploited or to being attacked. On top of this, the actual animals within these systems are not being protected by these legislations, potentially resulting in decreased welfare from attacks that may target them. There are different views, but we consider animals as more vulnerable creatures and we believe some of the SP and safety risks can have a differential impact on them. In addition, animals can be close to children, the elderly, and people with special needs who also are considered as vulnerable groups. Therefore, any technology dealing with animals should have the same level of SP and safety standards, if not more. Informed consent is an important aspect of current data privacy regulations such as the GDPR and CCPA, the application of this to animal-based technologies may need a slightly

different approach. As discussed before, the focus of protections should be on those human users interacting with these systems either directly or indirectly. Consent should be obtained via these human users who own these devices. Animals are unable to consent, so cannot consent to data privacy practices and we view this concept outside of the scope of this PhD work.

With regard to farming data, these systems typically do not collect any user information. However, it could be argued that the data of animals directly refers to their livestock owner [78]. Some of the farming systems focus on collecting data regarding the building environments. This data will likely be affected by the people working on a farm and therefore may capture some information about them. As well as this, the data and information about the farms collected by these systems is private to that farm and, as such, should be protected.

Security may also be more of a concern for farms and the systems used within them. Given the significant size of this industry, as a critical national infrastructure [117, 4], and the rapid growth of these technologies, security and privacy must be considered when designing systems for it. Some recent work such as [9] has been initiated by the sector to take these concerns into consideration, analysing possible risks to the industry, however, further work is necessary to fully understand and prepare for these risks.

The UK government has recently started training farmers about cyber threats, as they are seen as 'a significant threat to businesses' [73], showing an increased concern in this area. This also suggests that farmers may not be aware of the security and privacy risks that could be present in the technologies that they use. Given that one of the farm-based applications was found to have security issues, farmers should be made aware of the potential risks that these applications may bring. This will allow them to hopefully avoid using applications that could endanger their farms' security and privacy. By informing them of the possible risks, they may take further precautions before implementing a new technology into their farming systems.

3.6 Chapter Summary

The work within this chapter provides a security and privacy analysis of 40 animal-based apps (20 pet and 20 farm). The apps are used to interact with systems designed for use on or around pets and farm animals. We make use of a range of tools to perform static, dynamic, network traffic, and privacy policy analysis on these apps. We additionally perform a short review of the legislation surrounding animals and

the data collected about them, finding little in the way of protections that may have benefited the humans around these animals.

Our results showcase a serious security vulnerability that leaves the user's login details, amongst other account details in two of the apps, exposed and visible to anyone viewing the communications in three of the apps during the user's authentication. After communicating these vulnerabilities to the companies responsible and upon retesting, the two companies who responded to our communications had fixed this vulnerability. Poor privacy practices were additionally observed, with tracking services being communicated with prior to users being able to consent in over half of the apps (a violation of the GDPR).

These findings clearly show that the security and privacy of these systems are not the main focus during their design, with various examples of poor and outdated practices that leave the user's data exposed or do not effectively gain consent during this login and authentication step. Focusing on the security issue, we look to propose a solution that may be used to help secure the initial identification of IoT devices, such as those used on animals. This system would act as a precursor to authentication and should be secure but also easy to implement and simple for the end user to execute.

As discussed within our literature review, protecting access to the accounts and systems holding this data is of particular importance to those working with agritech systems, with concerns around misuse and misrepresentation [4]. As for pet devices, they were found to capture more data about the human users than their pets [132], and so this data must be effectively protected, starting with a secure and usable authentication system in order to connect devices that may be able to read or input data. This proposed identification system would work towards securing an aspect of these systems that we have found to be lacking.

Chapter 4

Sensor-based IoT Identification

In this chapter, we describe the process of designing and testing a motion-based identification method that can be used by IoT devices, such as animal technologies, as a preparation to authenticate. These devices typically have low-power capabilities/limited battery and minimal interaction methods, e.g., no screen or password input method. We cover the design of the system and the possible threat model it should protect against, the technologies used, the data collection process and the applicability of the final proposed system.

4.1 Chapter Introduction

With animal technologies, and the systems they send data to, becoming more commonplace in peoples' households and on farms, it is clear that the secure communication of this data is necessary. All stages of communication undertaken by these devices must be secure in order to effectively protect the user and even the animals. However, given the use case of these animal devices, they are likely to have limited resources in terms of processing power and battery life.

One stage of communication that is vital to be done securely is the identification stage, when the animal device (e.g., the smart tracker on a cow's neck) is connected to another system prior to sharing or allowing for the manipulation of the stored data. This is for the devices to know that the person initiating communication is the one expected, i.e., the farmer trying to connect a motion tracker to their larger system instead of a potential attacker/eavesdropper who may also want access to this system. To ensure the correct person is the one attempting to connect, identification methods may be used, typically relying on a piece of shared information known to the person attempting to connect. This could be something such as a passkey or a

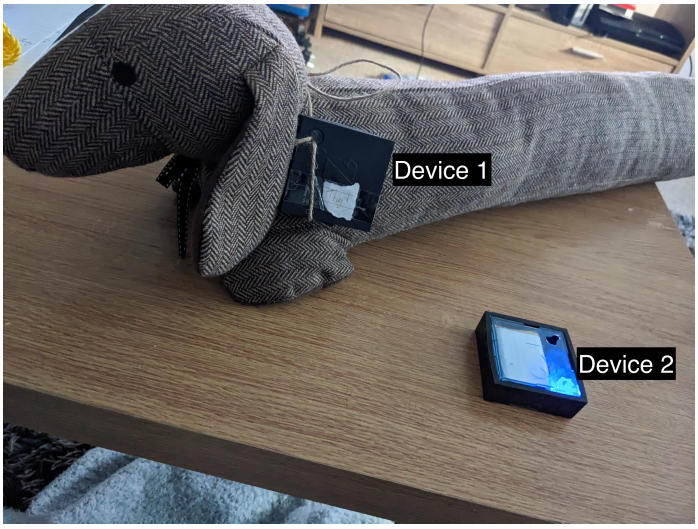

Figure 4.1: Example of tested orientation setup. IoT Device 1 is secured to a dog-shaped object and IoT Device 2 is tapped against it. This is a demonstration setup and we did not use it for our final data collection. Device 1 here would represent some form of animal tracking device; Device 2 would be the farmer/pet owner's device. The two devices are tapped together to generate a piece of shared knowledge.

one-time passcode. However, these forms of shared knowledge may not always be applicable to certain IoT devices with limited modes of interaction.

The purpose of our proposed system is to be able to generate a piece of this shared knowledge between two IoT devices to use for identification, that cannot be easily duplicated by the above-described attacker. This looks to take advantage of the built in motion sensors commonly present within IoT devices, such as animal-based devices. This would bypass the need for any sort of manual passcode entry that may not be possible on IoT devices (without having to introduce additional devices).

Previous research has looked into the use of motion data to authenticate mobile phone NFC payments using these motion sensors to prevent mafia and MiTM attacks [66], as well as other studies on motion-based authentication/fingerprinting covered in Chapter 2.6. However, the ideas in these work have not been tested on resource-constrained IoT devices. This work looks to fill this gap, highlighting the possibility of tapping-based identification and authentication mechanisms in resource-restricted IoT devices that may be used on animals, as well as in other areas of IoT, e.g., smart homes.

Our approach uses the accelerometer data of two IoT devices, when tapped together, comparing various features of the motion 'signals' to identify whether they are from the same tapping event. Previous works, such as those by Mehrnezhad et

al. [66], Gurulian et al. [40], and Wang et al. [134] have shown the effectiveness of using the accelerometer in devices for comparing readings involving vibrations. This will allow for the verification that each of the devices is the one that the other devices is attempting to connect to, with an eavesdropper unable to match this level of similarity.

In this chapter, we propose a motion-based identification method for resource-constrained IoT devices with limited interaction methods. We test the viability of comparing motion sensor data captured by two devices when tapped together. Our results show that there is promise in this area, achieving an equal error rate of 3.5% across 100 samples compared to one another. We hope that this work will help to inform the development and real world implementation of motion-based authentication for IoT, providing insight into its possible effectiveness, as well as discussing areas of further improvement and future work.

4.2 System Design

In this section, we present an overview of our system and describe the threat model.

Our proposed system would act as an identification mechanism for resource-constrained devices with limited interaction methods, being a precursor to authentication. We highlight the possibility of utilising the motion sensors present within many IoT devices (accelerometer), particularly those used on animals to generate a shared piece of information. Making use of these sensors, the user would tap two IoT devices together, generating similar motion data patterns across the two devices. These motion patterns are then processed and can be compared against one another to verify that the two devices trying to connect to each other are the devices being tapped. Further details on the specifics of this preprocessing signal comparison are discussed later within this chapter.

When first connecting two IoT devices, neither device will be able to fully trust the other. There will be no shared information or key enabling the two devices to trust that the other is the one they want to communicate with. This fact may leave the devices vulnerable to some form of man-in-the-middle or relay attack, in which a malicious party may intercept the communications and pretend to be one of the valid devices.

One common form of shared knowledge is a password, which the user may learn from a source outside of the devices or from one of the devices; with which they then communicate with the devices. This would require the user to be able to input the

password directly into the device or communicate via some other system, e.g., an app, introducing more possible points of vulnerability to the process.

Our system looks to utilise a matching snapshot of information that can be detected by the two valid devices, so that they may share a piece of common knowledge known only to them. This information should not be easy for an attacker to duplicate or gain access to, even if they are in a similar or the same environment. Many devices designed around use on animals have additional requirements, compared to regular IoT devices, such as a need for increased durability. Given this, they typically lack any real means of input method on the actual device, apart from maybe a button. In our proposed identification method, the user/users authenticating the devices would have physical access to both devices and can freely move one or both around. Similar to the work of Mehrnezhad et al. [66], this system should help to provide protection against man-in-the-middle attacks operated by someone in close proximity to the user. The feasibility of such attacks in an NFC payment-based scenario has been demonstrated by Drimer et al. [23].

The attacker/eavesdropper is able to be in a similar environment nearby to the actual valid user/users, where the use of other sensor information, e.g., environmental sensors would therefore be unable to protect the valid users. The attacker would be looking to eavesdrop on/intercept this initial identification process, allowing for the impersonation of a valid user, and enabling further attacks against those using the IoT devices. Motion-based authentication methods have been proven to be robust against this form of attack, where the malicious party is able to directly observe the motion-based collection process [134]. Meaning this identification process should aim to be able to operate even when an attacker is able to view the identification process. Whilst this system aims to assist in protecting against remote attacks, we do not claim to be secure against those attackers with direct physical access to the devices and view this as out of scope for the proposed system.

As discussed by Wang et al. in [134], a motion-based alternative to a passkey or pin would also potentially be a more accessible option, being easier to use for those with visual impairments. Tapping-based authentication has also been found to be effectively usable in user studies ([66, 134]), even finding that these systems rank as more usable than standard authentication methods).

IoT Device 1 **Nordic Thingy 52**	IoT Device 2 **Nordic Thingy 53**
	

Table 4.1: The two devices used to collect motion data when developing the identification system. IoT Device 1 - Nordic Thingy 52 (Left); IoT Device 2 - Nordic Thingy 53 (Right)

4.3 Proof of Concept Implementation

In this section, we explain how we implement this system, run the experiments, and collect data.

4.3.1 Experimental Setup

Device Type 1 - Nordic Thingy 52: We originally looked to use the Nordic Thingy 52[1], an IoT prototyping device containing a range of sensors, as seen in Table 4.1 (left). This includes an accelerometer, gyroscope, and magnetometer, allowing for a range of motion data to be collected. The devices are also capable of Bluetooth communication, allowing for the transfer and collection of this data via a laptop. Interacting with and collecting data from these devices is done via a locally hosted web page using HTML and JavaScript to call on the sensors.

In order to collect this motion data, we adapted one of the provided JavaScript files designed for interacting with these devices. This code called on these sensors, displaying the motion results of one device on the screen. Our first adaptation allowed for the connection and collection of data from a second device at the same time. This data was then added to an array to capture the overall motion of the tapping event. Within the JavaScript code, this data was then stored as a .csv file and made downloadable via a hyperlink on the hosted webpage. The results of when collecting data from this older device gave limited performance for the identification algorithm.

[1] www.nordicsemi.com/Products/Development-hardware/Nordic-Thingy-52

Because of this, we test our concept on a later version of this device.

Device Type 2 - Nordic Thingy 53: After the results with the Thingy 52 we decided to test a more recent version of the Nordic Thingy devices, as seen in Table 4.1 (right). The Nordic Thingy 53[2] is the step up from the 52, a more recently developed IoT prototyping platform making use of more recently developed sensors. Like the 52, this device contains a range of motion sensors, including an accelerometer, gyroscope, and magnetometer.

A large focus of the 53's design is around its use in prototyping machine learning-based projects, with these devices being used to capture the data used to train models and then later test them. An example of this being to capture hand motions while holding the devices, allowing for the training of a system to recognise and report back the specific motions being performed. Given this design focus, there is an online API that enables the easy collection of data from one device at a time. This involves the Thingy 53 being connected to a nearby mobile device via Bluetooth. This mobile device is then connected to the API, which is open on and being interacted with via a laptop. All collected data is sent from the Thingy 53 to the phone, with this then being relayed to the online API. The laptop is used to initiate the data collection from the device, as well as to view, manage and download the results.

Given that two of the Thingy 53 devices are needed for our setup, it was necessary for two lots of each device in the previously described setup to be used. This means that 2 Nordic Thingy 53s, 2 Pixel 6 Pros, and 2 laptops communicating with the API were all needed in the collection process. For the API aspect, 2 separate accounts were necessary to enable this simultaneous data collection.

Pixel 6 Pro: For the collection of data from Device type 2, mobile devices were needed as an intermediary. For this, we used two Pixel 6 Pros, each connecting to one the the Nordic Thingy 53s via Bluetooth, using the nRF Connect for Mobile app [3]. Both mobile phones were completely up to date, with no alterations made to how they function.

MATLAB was used to preprocess and process all of the tapping event data. This included importing the data as tables and calculating the magnitude of the x, y, and z axis, as mentioned above. MATLAB was also used to run the signal comparison

[2]https://www.nordicsemi.com/Products/Development-hardware/Nordic-Thingy-53
[3]play.google.com/store/apps/details?id=no.nordicsemi.android.mcp

methods, along with the testing of all of the possible input variables, making use of the signal processing toolbox, as well as the parallelisation toolbox in order to speed up the processing time. All work done on the collected motion data, after capture, was performed within MATLAB. Examples of the code used will be discussed and displayed below.

4.3.2 Tapping Process

Data Collection

In this section, we discuss the process of collecting the data within the tapping event, as well as the differences in collecting the data for the two different devices and the steps needed to collect data with them.

Participants and Recruitment

To ensure the validity of the developed identification system in a real-world environment, multiple data sets (tapping events) were collected for a participant, as well as across a range of different participants. Although we do not look into the possibility of user identification within this work, collecting these different data should account for and prove the applicability across differences in the motion data produced by an individual and across different people.

We collected data from a total of 25 participants, collecting 10 samples from each. Participants were recruited from multiple sources. The first set was recruited via friends and family, with the remaining participants being recruited within our university department, as well as with the help of Dr Matthew Leach and those within the Comparative Biology Centre at Newcastle University.

Each user that taps the devices together does so in a slightly unique pattern, with these differences varying between users, as seen in Figure 4.2. We collected data from 25 participants to ensure the effectiveness of our system no matter the user. These user-specific characteristics within these patterns may additionally allow for the development of this system to fingerprint specific users, allowing for a more secure pre-authentication protocol, and possibly enabling the adaptation of this system to be used for authentication purposes.

Each participant was given a brief description of the tapping process, with a demonstration of what they needed to do, as seen in Figure 4.3. Any mistakes during the process, e.g., tapping too many times or not enough, were simply repeated. Any

erroneous data was deleted. Aside from this tapping data, the only other data collected about our participants was their names, in case further contact was necessary for following up on these results.

Device Orientation

Prior to the involvement of the participants, different orientations of the devices during impact were tested, where for each instance, the two involved devices are positioned in the same way. For example, tapping the base of the two devices together, the tops of the devices, or matching sides. A more unique example of a setup we tested, meant to mimic a device being on an animal is shown in Figure 4.1. This was necessary for the Nordic Thingy 52s (IoT Device 1), where a protective rubber casing covered all but one side. For both of the devices, the base was tapped together, as this gave the clearest signal. An example of the actual orientation can be seen in the video linked in Figure 4.3

The Tapping Event

For both types of device, the actual tapping event was performed in the exact same way by the participants. As seen in figures 4.3, the two devices being used in the tapping event started flat on a table in front of the participant. At this point we ensure the devices are connected to their respective systems and ready the participant. The data collection is then started, with the participant being made aware when it has begun.

At this point the participant picks the two devices off of the table, raising them slightly and orienting the bases of the devices towards one another. The participants then hit the two devices together, immediately pulling them back apart. This collision was repeated three more times, totalling in four taps for the one tapping event. Once these taps are completed, the participant then places the two devices back down to their starting positions, base facing down and flat on the table. Each tapping event typically took no longer than a few seconds. This total process was repeated ten times per participant, as seen in Figure 4.3.

Any mistakes made, e.g., tapping too many times or a setup issue, were simply discarded with an additional tapping event being captured to replace this.

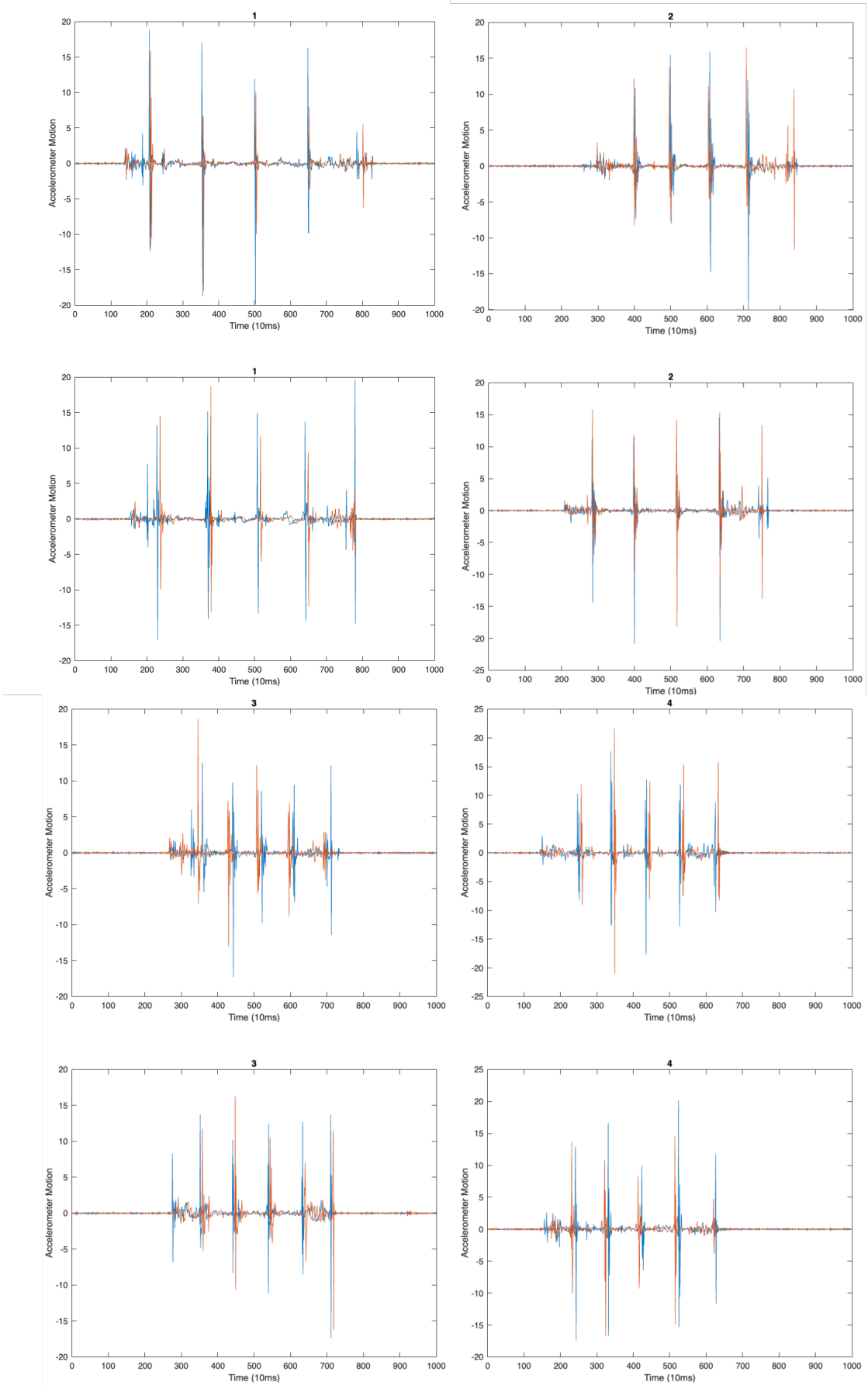

Figure 4.2: Examples comparing the patterns among and across participants. The number at the top corresponds to the participant number.

Figure 4.3: Pictures of example shown to participants, demonstrating how the devices should be tapped together for a tapping event. Full video of this example can be seen here: https://youtu.be/OPdEQI0uJo8

Device Type 1 - Data Collection

1st Iteration - Using the hosted web page, each device was connected one at a time via Bluetooth. Upon connecting to a device, they begin to start transmitting their data to the laptop, with these readings being displayed on screen. With this device transmitting data, the instance array also begins to fill up. The second device is then connected and begins to transmit data, with this also being collected and stored in the array. From here, the tapping process is started, capturing the motion data of the devices throughout, as explained above.

Device Type 1 Alignment Issues - Given that one device is connected before the other, data collection would begin earlier for one device than the other, as seen in Figure 4.4. We looked to compensate for this by adjusting the captured data and aligning it based on the position of peaks of the signal (ref example) within Matlab using the 'findpeaks' function. However, this process presented many issues, with otherwise well-matching data not always matching in peaks, meaning we were not able to automate this alignment process across all data.

Removing the Gap - To remove this gap in collection start time for the motion data, a button was added to start the process. Prior to the pressing of this button, none of the transmitted data is stored to either of the instance arrays. This allows for both devices to be connected and transmitting data prior to the tapping instance. When ready, this button is pressed and the data of both devices begins being stored at the same time. Using the web page, each device was connected and began to transmit

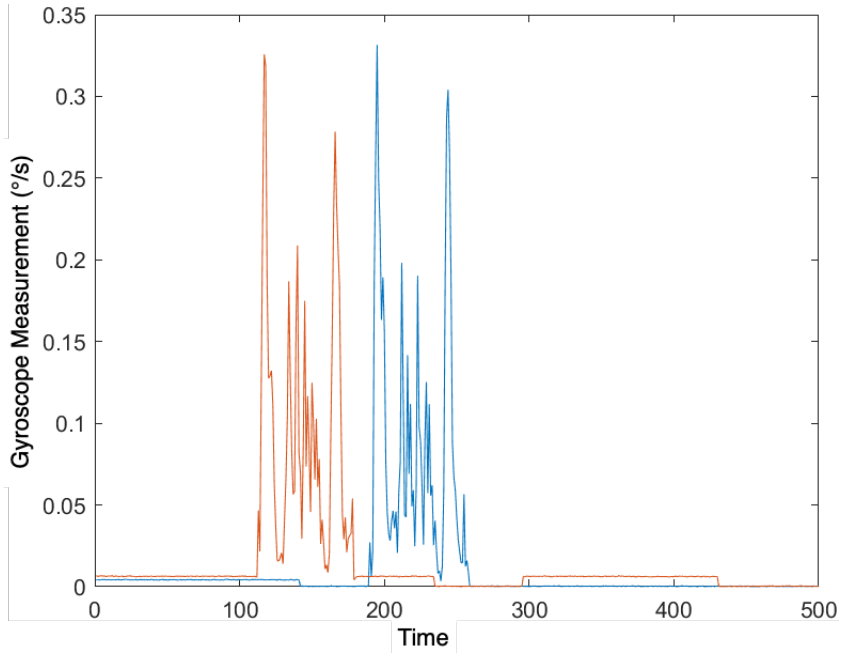

Figure 4.4: Comparison of the two devices' (IoT Device 1) gyroscope data during a tapping event. Data has not yet been aligned on the x-axis, though the similarities show promise for comparison.

data. To start, the button was pressed and the tapping process was completed. Once complete, the files containing the instance arrays of each device were downloaded. The no longer present differences in the alignment of the two signals can be seen in Figure 4.5, showing that no further alignment is necessary.

Device Type 2 - Data Collection

We used a similar format as our second iteration of the Thingy 52's data collection. The laptops connected to the API were used to initiate the data collection process at the same time. Once the devices have begun collection, this is communicated to the API and a blue light flashes on the devices as well to signal this. At this point, the participant is informed to begin the tapping process.

This process may involve pauses between the taps, as well as after picking up or before putting down devices, depending on the preference of the participant, with participants being encouraged to tap it how they want and try different speeds if they want. After this instance of tapping, the remaining time in the data collection period is waited out and the readings are confirmed to have been collected and communicated by checking for a new reading within the API. A set time frame of 10 seconds was used per tapping instance to ensure that all tapping events would fit within the recording

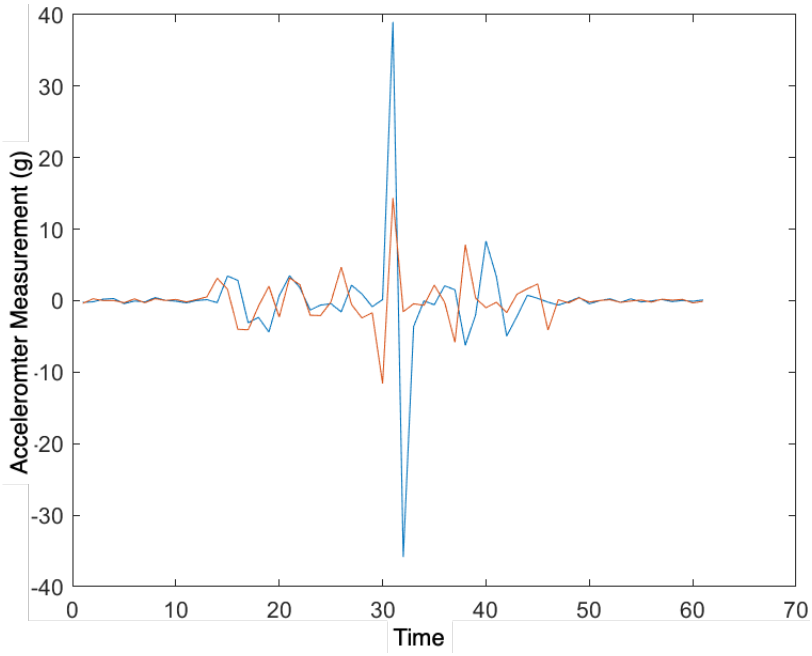

Figure 4.5: Comparison of the two devices' (Device Type 1) accelerometer data during a tapping event. The similarities show promise for comparison.

time frame (with some participants tapping slower than others). Typically, however, this extra time was not needed for the majority of the participants but ensured the comparison of all signals without extended processing of the data. This process is then repeated a total of 10 times per participant, with very little turnaround time between each instance. This allows for the process to take around 5 minutes and no longer than 10 minutes in the event of some results not being collected properly. In these cases, the instance is repeated.

This data is downloaded via the API as a .cbor file. These files were then grouped and placed into a folder per participant. A short Python script was run on the folders to rename the files, ensuring that the matching tapping events may be correctly matched later during the processing of results, as well as to speed up further processing of the files. From here, another short Python script was run on each file to convert the data to a .csv file, for use within MATLAB (preprocessing and running/testing the signal comparisons).

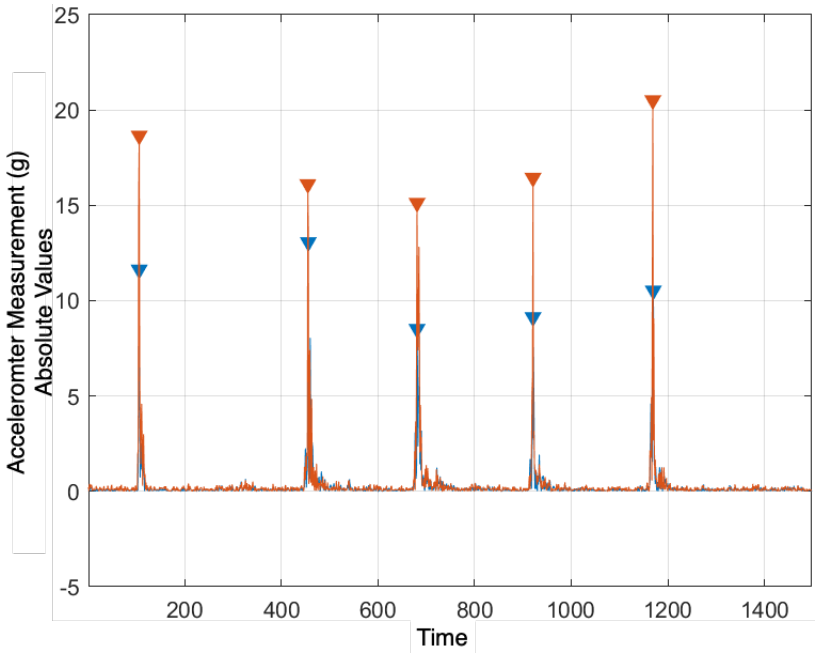

Figure 4.6: Comparison of the two sensors' (Device Type 2) motion data during a tapping event. The data has been preprocessed, calculating the differential and then the absolute, highlighting the similarity of the data captured by the two devices.

4.3.3 Signal Processing

Pre-processing

We try to limit the amount of processing done on the signal data prior to the actual comparisons, given the lower-powered IoT devices this system would be aimed at. The actual data collected includes the x,y, and z-axis readings from the motion sensors (accelerometers). To 'combine' these data points and capture the overall motion of the devices, we calculate the magnitude, as seen in Equation 4.1 (e.g. [61]).

$$n = \sqrt{x^2 + y^2 + z^2} \tag{4.1}$$

For Device Type 1, given that we had more control over the actual collection process, we calculate the magnitude shortly after obtaining the x,y, and z values before saving the data to the array. For Device Type 2, this calculation was performed within MATLAB after importing the signals within the system, with these new values being saved in a fourth column, after the x,y, and z values. Various additional alterations were also made to the data, with the effects of these being tested and compared against each other and the results on the raw data. These include calculating the derivative of the signal data ($y = \frac{dy}{dx}$), which is calculated in MATLAB with:

signal1 = diff(signal1). We also calculated the absolute values of the data with: **signal1 = abs(signal1)**, and quantisation (discussed more within Section 4.5). Unlike in [66], we do not perform any sequence alignment processes. Though this could be used as an additional stage in future implementations, we found our system was able to produce effective results without the need for this stage and that these methods could be inconsistent when dealing with more varied tapping sequence patterns, i.e., from more participants.

The derivative of the signal data calculates the rate of change in y with respect to the change in x across the signal. This can help to make changes in the signal more prominent, however, with the risk of increasing the amount of noise. By looking at the amount the signal changes, instead of the direction moved (which is reflected in the raw data), the motion signals of the two devices are better aligned. This is due to the fact that the devices are moving in opposite directions when being moved back and forth during the tapping event. The effect of this process can be seen in Figure 4.5.

The absolute values of the motion signal effectively flips all negative values produced by the derivative calculation. This can again help to remedy the different directions the devices are moving and can be useful for peak detection, with previously negative peaks being mirrored and level with the positive peaks. The effect of this process can be seen in Figure 4.6, in which this preprocessing results in near identical signals. However, as with all preprocessing methods, this process removes some of the possible uniqueness present within the raw data, possibly increasing the likelihood of false positives when comparing two signals.

Signal Comparison

The motion data produced by the tapping of the two IoT devices are represented as signals from each device. There are many methods of comparing and processing signals, capturing different aspects of them. Our initial comparisons of these signals involved simply overlapping them for visual analysis. We used this to manually compare the effectiveness of the two device types studied, as well as for testing different setups.

For the final signal comparison used to authenticate the devices, we look at the correlation coefficient, the coherence (e.g. [61]), and the energy difference (e.g. [66]). The correlation coefficient was found using the **corrcoef** function within MATLAB. Similarly, the coherence was found using the **mscohere** function, however, this re-

quired an additional sum of all the generated values as seen in Equation 4.2. The energy difference involved calculating the energy of each signal as seen in Equation 4.3 and then subtracting one from the other and taking the absolute value to remove negatives, as seen in Equation 4.4. Unlike in [66] we did not calculate the peak gap difference. We found the implementation for this to be temperamental (similar to sequence alignment) and was unnecessary to obtain effective EERs. Future implementations looking to be able to cope with a greater amount of comparisons may look to implement this feature into the signal comparison calculation. We also avoid the use of machine learning methods for this signal comparison and identification, e.g. [55, 40], as we want this pre-authentication process to function on resource-constrained devices.

```
cxy = mscohere(tab1,tab2);
[coherence,n] = sumsqr(cxy);
```
(4.2)

```
FrameLength = 10;
movrmsWin = dsp.MovingRMS(FrameLength);
energyPer1 = movrmsWin(tab1);
energyTotal1 = sum(energyPer1);
```
(4.3)

```
energyDiff = abs(energyTotal1-energyTotal2);
```
(4.4)

For coherence and energy difference, these values were then normalised, to give them equal weighting within the final comparison calculation, shifting their value between the range of 0 and 1. The normalisation involved dividing their value by the maximum possible value. The energy difference additionally needed inverting, with a lower difference correlating to higher similarity, this was simply done with the following MATLAB code: **energyDiff = 1-energyDiff**.

```
similarity = a*correlation + b*coherence + c*energyDiff
```
(4.5)

Like in the work by Mehrnezhad et al. [66], we apply weights to all of these

comparison values and combine them to get an overall similarity, this equation can be seen in Equation 4.5. We tested a range of weight values, testing all possible combinations where the total of the three weights is equal to 1. The weight values could each be between 0 and 1, and up to two decimal places.

This similarity value would then be compared against a pre-determined threshold value. If the value is below this set threshold, then the signals would be seen as being from the same tapping event. For our experiments, we tested a range of threshold values, with the value being between 0 and 1, and up to two decimal places. This range of threshold values was additionally compared with the range of weights, testing all possible values for these variables. The full parallelised version of the code can be seen in Appendix B.

4.3.4 Ethical Considerations

No sensitive data is collected by the devices within the data collection process, only the motion data of those specific instances, which cannot be used to link back to the participants in any way. This is expressed to the participants prior to collection when obtaining consent. Visualisations of the collected data (graphs) can be displayed within the API, with examples of this being occasionally shown to the participants to demonstrate the type of data collected within the process.

Participants' initials are used in the naming of the data files for clarity in implementing the data and later comparisons, however, this is unlikely to be able to be linked back to the participants and is the only personal data collected. The initials also enable us to keep track of who we have collected data from in case further demographic information was needed for comparisons, we could then request to use this from our participants. These initials will not be given in any results or writing shared about the work to ensure the privacy of our participants.

4.4 Results

Here we show the results of the proposed signal comparison and pre-authentication system. We focus on the equal error rate (EER), with a lower value of this representing a system that is less likely to admit attackers and reject valid users.

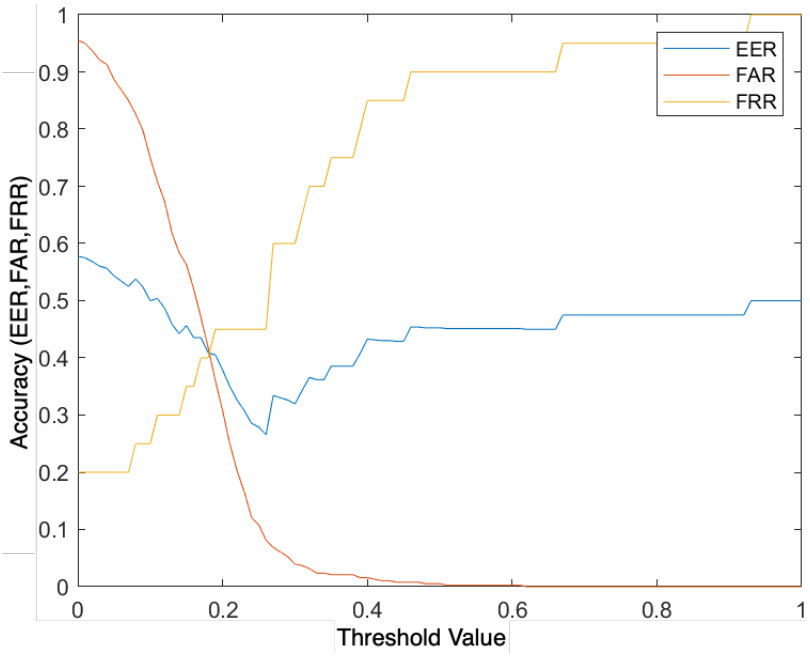

Figure 4.7: Nordic Thingy 52 -View of error rates when using the best range of input variables. Results are shown across the tested thresholh values (0-1). Highlights poor performance with this setup.

4.4.1 Signal Comparison Overview

Device Type 1 - Nordic Thingy 52

We were unable to obtain an EER lower than 25% when using this setup, as seen in Figure 4.7. These results are from experiments using only 10 samples. Given these poor results, we tested a newer set of devices (Device Type 2).

Device Type 2 - Nordic Thingy 53

When testing the motion data for this device type, we compared each of the tapping signals against their corresponding signal, as well as a range of unrelated signals from other tapping events (all other samples in the data set). For these comparisons, a total of 100 tapping signals were used, resulting in just short of 10,000 comparisons overall (9900). Given this large amount of data being compared, along with additional running of all possible variables for weights and threshold; larger datasets were unable to be ran on MATLAB. However, we believe that the extent of these comparisons are able to effectively justify the use of this system in the real world.

Given the data collected from our participants, 25 lots of 10 samples of tapping data (250 total), we used a mixture of this data set across a range of experiments.

Starting with the original 10 participants, we set up and performed experiments on this data set of 100 tapping samples. We further tested our next set of 10 participants amongst themselves, as well as these two sets mixed together (using 5 samples per person to remain at 100 samples). Additional experiments were performed across the full set of 25 participants, using the first 4 samples per person for consistency.

Our comparisons involved testing all possible values for the weights, as well as all possible thresholds from 0.000 to 1. This resulted in a total of 5,077,270 comparisons. This is clearly far more than an identification system would actually need to run, and is done to test the robustness and feasibility of the proposed system. Given the large amount of comparisons, this led to very long run times within MATLAB. To aid with this, parallelisation was implemented within the MATLAB code, making use of MATLAB's available parallelisation features. This cut the run time down from roughly 1 week to just under 2 days.

Our early comparisons and tests of the signals involved just 10 tapping samples being compared to one another (either from one person or multiple). Within these smaller experiments, the system was able to consistently achieve an equal error rate (EER) of 0% across multiple sets of 10 samples.

When increasing the number of compared samples, the system saw a slight dip in performance. The system was able to obtain an EER of 0.035 or 3.5% when comparing a set of 100 tapping samples. This EER is achieved with an FAR of 3% and a FRR of 4%. This would mean that an attacker would only have a 3% chance of matching the legitimate user's tapping signal. The slightly higher false rejection rate is fine, as this would just mean a 4% chance that a valid user would need to reattempt the identification process, impacting only usability and not security.

If a lower FAR is desired, for the purposes of a more secure, albeit less usable system, the threshold can be adjusted, raising the FRR instead. Examples of this can be seen in Table 4.2, showcasing some of the best FAR values where the EER is below 10%.

This best EER was achieved with weight values a=0.02, b=0.87, c=0.11 ; where a,b, and c are the weights for the correlation coefficient, coherence, and energy difference respectively. The threshold used to achieve this best range of values is 0.22, where possible similarity values are between 0 and 1, and the threshold is up to 3 decimal places.

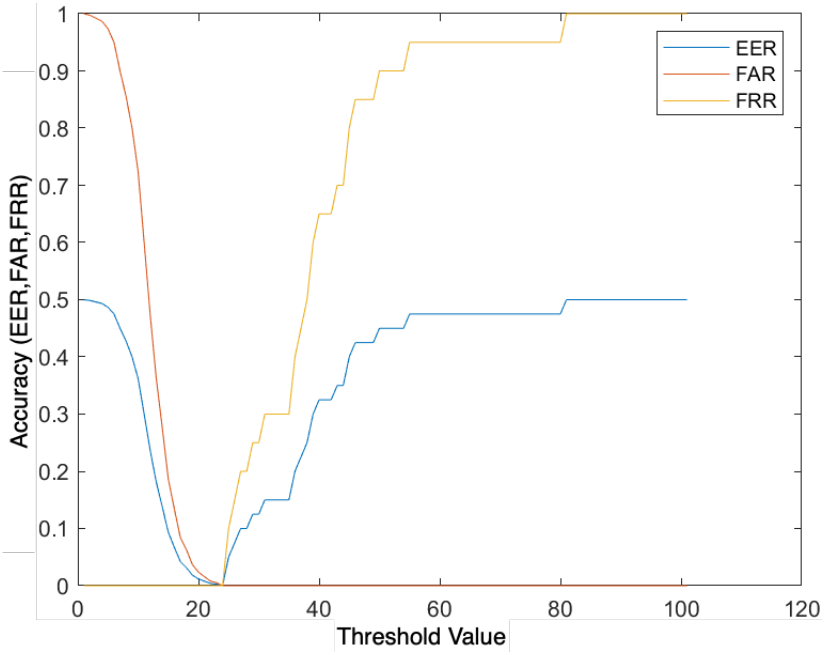

Figure 4.8: Thingy 53 - View of error rates when using the best range of input variables, with the x-axis being all possible thresholds. Results show the possibility to achieve an EER of 0% when comparing 10 samples.

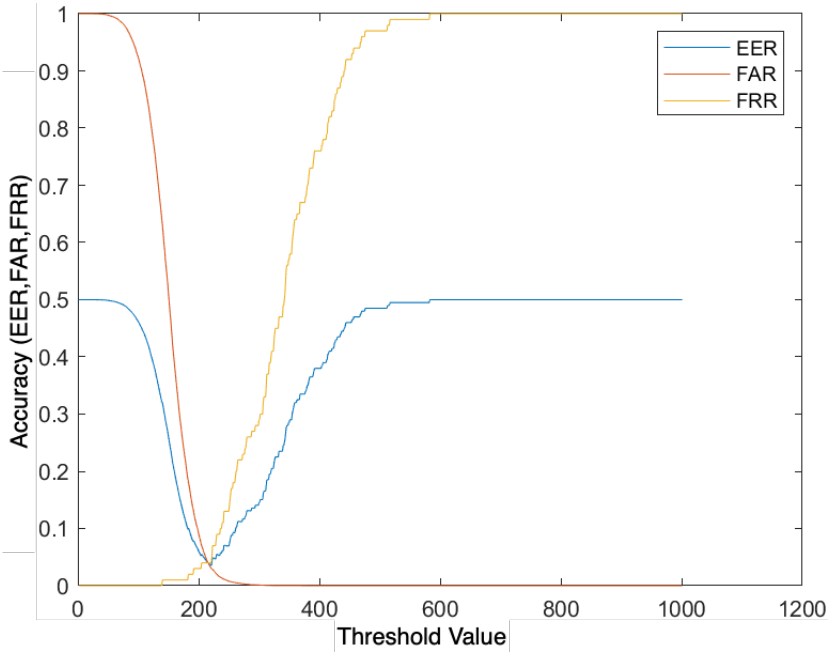

Figure 4.9: Thingy 53 - View of error rates when using the best range of input variables, with the x-axis being all possible thresholds. Results show the possibility to achieve an EER of 3.5% when comparing 100 samples.

4.5 Implementation of Quantisation

While our main results do not rely on quantisation, we performed further experiments to show the potential use of our proposed system in real-world commercial applications. Quantisation is the process of transforming a signal by mapping its data points into a smaller set. Here we look to transform each data point into a binary value, allowing for the signal to be represented as a binary string of data.

This altered representation of the signal, which does not contain any double values, may allow for less powerful devices to process and transfer this data. Having the signals in this binary format also allows for the use of Hamming distance as a measure of similarity between two signals.

Implementation

We adapted our previous main method for testing input values from our signal processing method. This calls instead on a quantisation method and an adapted version of our error rate method. The error rate method here just needs to check whether the calculated hamming distance is above or below a given threshold; reporting back whether each result is a false accept or false reject, and allowing for the equal error rate to be calculated.

Variables

Only two variables were altered at first, the resolution and the threshold. With regards to quantisation, resolution refers to the number of bits used to represent a single data point. 1 bit resolution would represent a data point as a 0 or 1, depending on whether its value is less than or greater than half of the maximum value. 2 bit resolution would represent the data as 00, 01, 10, or 11 and so on. We tested up to a resolution of 10 bits in some instances.

The threshold looks to accept hamming distance results that are below a set amount and reject those above it. The hamming distance result is kept as a value in the range between 0 and 1, meaning the threshold is also within this range. A variety of possible threshold values was tested within this range, incrementing by 0.01.

Multiple Resolution Quantisation

Given the varied lengths of the tapping events within the collection time frame, some tapping events would only take up a portion of the overall collected data, with many

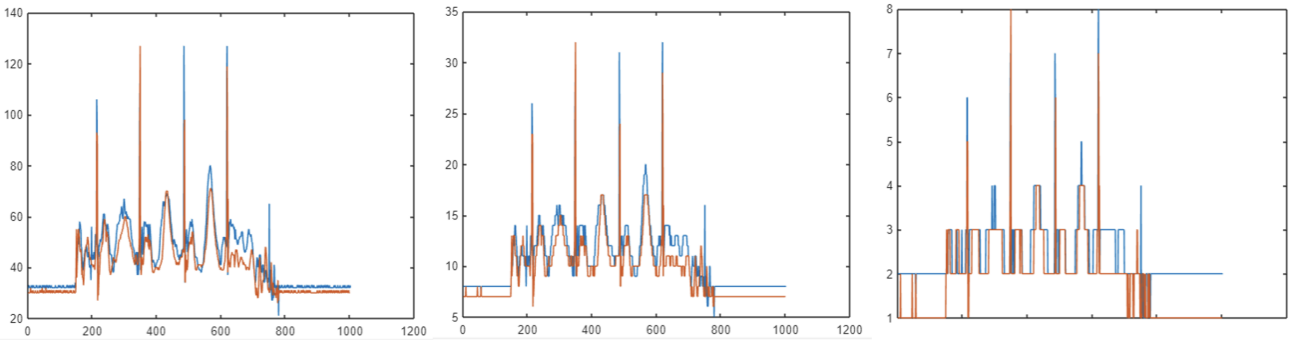

Figure 4.10: Visual examples of the effects of quantisation on the same tapping instance. **Left** - 7 bit quantisation largely retains the original signal. **Middle** - 5 bit quantisation more clearly shows some of the details being lost whilst retaining the original shape of the signal. **Right** - 3 bit quantisation again retains most of the general shape, however, with much less accuracy and the introduction of dips that were not present in the original signal. Y-axis represents the quantised version of accelerometer motion data. X-axis shows time.

having 'spare' data at the end that did not reflect the actual event. With this, not all of the total data gives as much useful information about the tapping event. To account for this, the signal was split into multiple sections, with different sections being quantised at different resolutions. We tested a range of values for the resolution used for each section with a focus on higher resolutions on those parts of the signal that include more of the tapping event.

Quantisation Results

Despite the promising initial visual impressions, we were unable to achieve close to a usable EER when applying quantisation to the signals. The best EER achieved when using quantised versions of the data was 28.89% on 100 samples, significantly worse than our previous best. We believe some of the reasoning for this may be an increased sensitivity to unaligned signals within the comparison method used with these new signals. As seen in Figure 4.10, the patterns are maintained at higher resolutions, so this is clearly not the issue with this approach.

Attempts were made to align this data by matching the peaks within the data. Whilst a promising solution, attempts at this were inconsistent given the variance in the data samples - which reflect the actual variance of real-world data that a system would need to handle. This resulted in multiple of the transformed signals being incorrectly corrected, drastically lowering their similarity to their matching tapping sequence.

EER	FAR	FRR
0.092626263	0.005252525	0.18
0.097626263	0.005252525	0.19
0.092828283	0.005656566	0.18
0.093030303	0.006060606	0.18
0.093131313	0.006262626	0.18
0.088181818	0.006363636	0.17
0.088282828	0.006565657	0.17
0.088484848	0.006969697	0.17
0.083585859	0.007171717	0.16

Table 4.2: Table demonstrating the possible compromises to FRR to improve the FAR. In this table, a value of 0.18 corresponds to 18%.

Despite an additional step of preprocessing, quantisation would make for an effective step in this sort of system, reducing the size of data that may be transferred and enabling simple comparison methods such as Hamming distance. We believe that further research should be performed to try and effectively implement this into our proposed identification method.

4.6 Discussion

4.6.1 Security Analysis

The results of this study demonstrate the applicability of motion sensors within a pre-authentication system for resource and input method-constrained IoT devices. Though the EER does reduce slightly in quality with a larger amount of samples being compared against, the EER of 3.5% is strong enough to protect those using the system whilst maintaining usability.

An attacker attempting to impersonate one of the participants of the tapping process would need to be within the short range in which this data would be transferred. They would then need to produce a tapping sequence close enough to the actual sample. In the case of this method, this would need to be done visually by the attacker, watching the motion of the legitimate users and then recreating this. Recreating an exact tapping pattern would not be easy for an attacker, particularly within the short time frame you would expect the identification process to take place.

The variance in possible tapping patterns may be further increased by introducing varied amounts of possible taps within a tapping sample, e.g., two taps or five taps. This would introduce additional randomness to the tapping samples, further increas-

ing the difficulty of a sample being replicated. As mentioned above, by adjusting the threshold of the system it is possible to prioritise the FAR or the FRR more. There are obtainable FAR values of less than 1%, with the trade-off being a FRR of just under 20%. The threshold and these resulting values can be adjusted depending on the system in which this identification method is being used.

As we mentioned earlier, physical access for an attacker is out of scope for the proposed system, with this enabling an attacker to generate their own tapping signals, rather than just observing and attempting to replicate. However, further measures may be implemented to protect against this form of attack, utilising MAC addresses and the UID of legitimate devices within the system to ensure only valid devices are being connected to. This additional layer of security is necessary if adapting this system as part of an authentication protocol.

4.6.2 Comparison to Related Work

To get a better understanding of our results, we compare them against similar studies looking at using motion sensors for authentication. Our EER of 3.5% is very close to that of these similar works. A gesture-based authentication system by Wang et al. [134] was able to fingerprint users with an FAR and FRR under 2.5%, with a best case FAR of 0.41%. When protecting against an attacker, the attacker was only able to bypass the authentication process 3% of the time. In a similar system, in which the user taps a smartwatch to a melody, [75], Nguyen et al. was able to distinguish the user from an attacker with an accuracy (EER) of 98.7%, with a best case FAR of 0.98%. For Lee et al.'s, system designed to recognise specific users, using the accelerometer, gyroscope, and magnetometer in smartphones, they were able to achieve an accuracy of 97.4% when using all of these sensors [55]. Our system is able to achieve similar results to this and only makes use of the accelerometer data collected by the device. Gurulian et al.'s vibration-based system compares the motion data between two devices after a series of vibrations [40]. While this system is able to achieve a very impressive EER of 0.001, this utilises machine learning, adding to the amount of processing and potentially making it not as applicable to resource-constrained IoT devices. The system proposed in Tap-tap and Pay, by Mehrnezhad et al., was able to achieve an EER of 9.99% when comparing motion data between two mobile devices (with one acting as a mobile point of sale terminal) [66]. This EER is achieved with an FAR of 0%, with all of the errors coming from false rejections. The work of Mayrhofer et al. ([61]), where two mobile phones are shaken in one hand was

Paper	Purpose	Sensors Used	Motion Type	EER	Best FAR
[134]	Fingerprinting/Authentication	Touch,Accelerometer,Gyroscope	Hand Gestures	< 2.5%	0.41%
[66]	NFC Payment Verification	Accelerometer	Tapping against device	9.99%	0%
[75]	Smartwatch 2FA	Pressure,Size of touch	Tap screen to melody	1.3%	0.98%
[55]	Fingerprinting/Continuous Authentication	Accelerometer,Gyroscope,Magnetometer	Holding/walking	2.6%†	-
[40]	Artificial Ambient Environment for data transactions	Accelerometer,Gyroscope,Gravity,Linear Acceleration,Magnetic Field, Rotation‡	Vibrations	0.001%†	-
[61]	Secure pairing of mobile devices	Accelerometer	Shaking	5%	0%
This Project	Identification	Accelerometer	Tapping devices together	3.5%	0.52%

Table 4.3: Comparing our results to those of previous motion-based authentication studies. - FAR values not specified. † utilising machine learning. ‡ one sensor used at a time (decided when ran).

able to achieve an EER of around 5%. This work looks to use this shaking motion for the secure pairing of mobile devices and is able to achieve an FAR of 0%, similar to the work of Mehrnezhad et al., with the 10% FRR being the only errors in the system. The results of these related studies can be seen in Table 4.3

From these results, we believe that our proposed system shows promise as a possible solution contributing towards IoT authentication, obtaining similar EER levels to other works. Additional improvements, applicable outside of this exact setup, may be implemented such as the use of multiple motion sensors, e.g., gyroscope as well as the accelerometer. As in Tap-tap and Pay [66], additional information may be drawn from the tapping signals, such as the distance between peaks. Given the greater number of peaks within our tapping process, this metric proved difficult to obtain consistently, we leave the possible addition of this as future work.

4.6.3 Applicability of the System

One key advantage of this type of system within authentication is its ease of use. The simple process of tapping devices together bypasses the need for a password/passcode to be entered and the potential user error that would be introduced. Previous studies have been done into the usability of tapping for authentication. In a study where participants tapped a phone screen for this authentication [59], they found this method to be comparable to PIN and drawing unlock methods both in terms of usability, as well as resilience to shoulder surfing. Similarly, Mehrenzhad, et al., found that those participants who tested their tapping-based system viewed the system as being faster and more secure [66]. Given the similar types of motion being used within this study, users of the system would likely feel the same, however, future work would be needed to test the real-world usability of an authentication system utilising this identification method.

The types of sensors used within this proposed method are incredibly common within IoT devices, particularly those used on animals. Accelerometers are used in devices such as activity monitors to detect the motion of an animal. Through using these already implemented sensors, this system can be more easily deployed into already existing devices, without the need for any hardware adjustments. However, the results of our Device Type 1 experiments show that older hardware does have its limitations, providing much less usable results compared to those of the updated model.

4.6.4 Limitations and Future Work

A clear downside to this type of identification/authentication is that the data transfer is being done out in the open, where the process can be visually observed by an attacker. Though it would be possible to take additional precautions to mitigate this, e.g., obscuring the devices being tapped, we believe this to be largely unnecessary. The unpredictable nature of the tapping process and the variance in possible tapping signals would make the tapping sample very difficult to predict or replicate fast enough to be of use.

An aspect of this system that requires further research is testing the performance when using two different types of devices within a tapping process. Differences in the motion sensors used within devices may result in signals that do not match as exactly as the data we tested. Work should be done to see if the effectiveness of the proposed system would be affected by this scenario and whether any mitigations can be employed.

Another possible direction for this work would be to look into the possible fingerprinting of users. Throughout this work, there were some visual differences between the samples obtained from the participants. It may be possible to use this tapping process in some way to verify/authenticate a human user based off of how they tap the devices together. Previous studies have looked into this motion-based fingerprinting, e.g., [75]. Like with those previous studies, this type of solution would likely require the implementation of machine learning methods and, as such, may not be as applicable between two resource-constrained devices.

4.7 Chapter Summary

In this chapter, we have proposed a mechanism for identification, that may be utilised by resource-constrained IoT devices, whose interaction methods are limited. Making use of the accelerometers commonly found within these devices (allowing for easy deployment), we test a tapping-based procedure to generate a shared piece of knowledge (the motion data). We make use of two IoT prototyping platforms (Nordic Thingy 52 and Nordic Thingy 53) to demonstrate the effectiveness of this proposed method.

Our findings show that this proposed system is able to obtain low equal error rates when comparing 100 different tapping samples, comparable with similar motion-based authentication systems, whilst using only one sensor type. The EER of 3.5% is comparable to that of other studies without the use of machine learning being necessary. This EER indicates an accurate system that can effectively protect the users, whilst limiting the amount of repeats necessary. Additionally, the system can be adjusted to accommodate the needs of prioritising a lower false acceptance rate and is able to achieve an FAR of 0.52%, again comparable with the related works. Future research into this pre-authentication method may include using additional sensor data and testing with more varied device types for its development into a full authentication system.

Given the results of Chapters 3 and 4, we need to gain a better understanding of how users interact with these systems and the concerns they may have. We have identified security issues in the user authentication stage of the apps related to these devices and proposed a usable solution to be utilised in the authentication of the physical devices themselves. Gaining insight into the user's concerns and views of these systems will help to shape any discussion around the future secure design of these systems. Additionally, this will give insight into the reality of possible security issues and the current methods they employ to protect themselves.

Chapter 5

User Studies of Security and Privacy of Animal Tech

In this user study chapter, we describe the process of designing and distributing our questionnaire. We give an outline of the participant's demographics, highlighting the range of participants involved in our study and we discuss the methods used to analyse our results.

5.1 Chapter Introduction

With these devices being used more and more on people's pets [104], the industry will continue to offer more solutions that are potentially not secure (as shown in Chapter 3) and expose the user to the risk of attack. A wide range of different devices are being used to help care for pets, which 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.

The owner's pet may not be the only target of attacks against pet technologies. Attacking these systems may reveal some of the potentially personal data that is collected by these devices. This collected 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.

Building off of our previous works in this thesis, we were interested in gaining more of an understanding around the users' perspectives with these animal technologies. Given the range of pet technologies accessible for purchase, the growth of this industry, and the possible security and privacy issues, we wanted to hear from the users of the

I) Demographics	II) Pets technologies	III) Risk-related questions
- User-related - Animal-related	- Usage - Pros and Cons	- Incidents, - Data access and potential attackers - Protective actions (general, pet tech) - Desired security and privacy features

Table 5.1: Overall design of the pet tech survey

devices/apps whether they have any concerns or had experienced an incident with these devices, e.g., an attack. We wanted to gain an understanding of their reasons for using these devices, their feelings towards them, as well as their concerns and understanding of possible attacks that may target these devices.

Few previous works have looked into this aspect of the user's concern regarding pet tech, with *none* also touching on the possible security issues and incidents. Given that these technologies are commercially available and being used routinely by pet owners, there are a range of possible insights to gain from learning about their personal experiences with these technologies.

We achieve this by performing a user study of pet owners from different countries, distributing the survey to roughly 600 pet owners across the UK, the USA, and Germany, with around 200 participants from each. We design and run a survey to better understand their point of view regarding the security and privacy of these devices. We ask a range of questions, covering the pet technologies in use, why they are used, the perceived 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 and ask for any security features they would like to see included.

We find that the participants use a large range of pet technologies, not just GPS and activity monitors and that their focus with these devices and the data they collect is more on the care/welfare of their pets and not data relating to them as human users. Our findings also reveal that users 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.

5.2 Survey Design and Distribution

5.2.1 Survey Design

We start the survey by briefly introducing the relevant technologies to the participant. As seen in Table 5.1, we then ask a short selection of demographic-based questions. 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."*

This is followed by a set of questions attempting to ascertain what technologies the participants use and for what purposes. These include the animals they use the devices on, the duration of the technology use, and the types of data they enter into these technologies. We then ask the participants to explain the benefits and disadvantages of using these technologies via multiple-choice and open-text questions.

The next section focuses on incidents involving these technologies. This includes any that they have experienced, are aware of, or believe may occur. We also ask who they believe has access to their data and who would be interested in performing an attack. These questions are a combination of listed items and open-text questions.

Finally, we ask the participant about how they protect their security, both generally and for their animal tech systems. We also ask who they believe is responsible for taking care of their security and privacy within these systems, using a combination of multiple-choice and open-text responses for each of these questions. Finally, we ask what security features they would like to see included and if they have any other comments, both of these being open-text.

The combination of open-text and multiple-choice for many of the questions was done to capture the participant's initial response and then aid them with some suggestions if they are struggling to come up with a response. The full survey can be seen in A.1.

5.2.2 Survey Distribution & Participants

To distribute our survey, we used Prolific[1], a user study distribution platform. Prolific pays its participants for their time, allowing for the rapid collection of results. Prolific allowed for the filtering of possible participants, allowing us to specify participants with a cat or a dog, as well as their country of residence.

[1] prolific.co/

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

Table 5.2: Participant Demographics. F: female, M: male, N: non-binary, one UK participant did not want to share their gender.

We distributed the survey to participants across three different countries (UK, USA, and Germany), receiving responses from 593 in total. We received 199 responses from the UK, 197 from the USA, and 197 from Germany. These countries were chosen as they had the most available participants through Prolific when applying our pet-based filters. Aside from country of residence, the only other factor taken into account when choosing the participants was whether they had a pet. We only sent the survey to people who have a cat or a dog, given that the majority of pet technologies are designed for them.

The mean age of the participants was 33.5, with the UK and USA participants being on average 36 and 35 respectively. This leaves the German average of 29 comparatively younger than the other two countries. In terms of 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 5.2.

5.3 Analysis Methods

For this paper, we have processed the collected data and represented the results through descriptive text as well as the use 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 [38]. 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.

5.4 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.

5.4.1 Pet Technologies Use

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"* to help keep their dog active. 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.

Data Collection Awareness

As seen in Figure 5.1 (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"* and *"Just movements and sounds"*. Pet health contains responses surrounding the capturing of pet health-related data, e.g., *"Dog Weight, Heart BPM, calories, exercise level..."*, as well as information relating to an animal's past treatments: *"medical information when they have last had treatment"*.

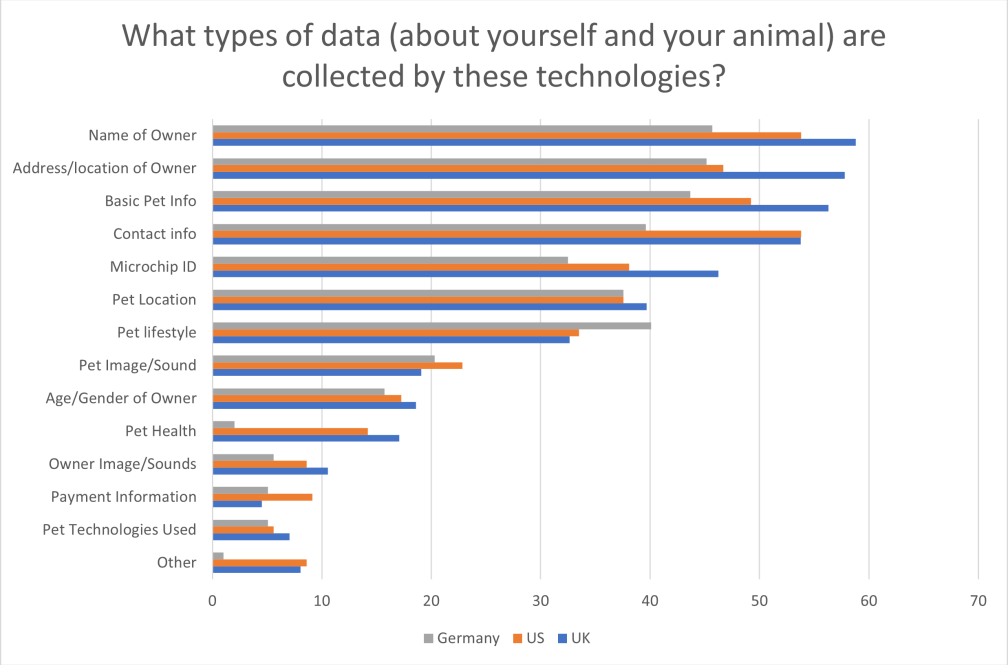

Figure 5.1: Percentage of participants from each country who believe that pet tech devices gather the following data.

Additionally, the participants mentioned the collection of information relating to the vet they use, as well as the appointments that they have with them (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"*, comparing these devices and their practices to the more typical devices that they would interact with.

Advantages and Disadvantages

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 5.3

Pet welfare here refers to the improved pet safety around *"prevent[ing] a pet getting*

Advantages of Pet Tech		**Disadvantages of Pet Tech**	
Easy to use	435	Expensive	319
Improve pet welfare	414	S&P 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		

Table 5.3: Perceived advantages and disadvantages of pet technologies.

lost", as well as monitoring the health of the pet and *"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, while also including the grouping/centralisation of the pet's data, 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"*.

For peace of mind, participants mention that they *"feel safer knowing where they are when out of the house"*, showing that GPS devices can help to reduce stress owners may have about losing their animals. It also includes the multiple responses around caring for or checking on their pets when they are away from their home, with a participant saying: *"Make sure she is safe and fed when not there"*.

Some additional advantages mentioned by the participants include *"more control"* and the benefits of data collection and use, i.e., *"Data may help science"*. Another participant mentioned a different type of practical advantage with *"dog stops barking when [the] device makes a sound"*, demonstrating alternative uses of pet tech outside of just welfare, safety, and convenience.

Disadvantages The main disadvantages identified were the costs involved with these devices, security and privacy 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 5.3.

'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*

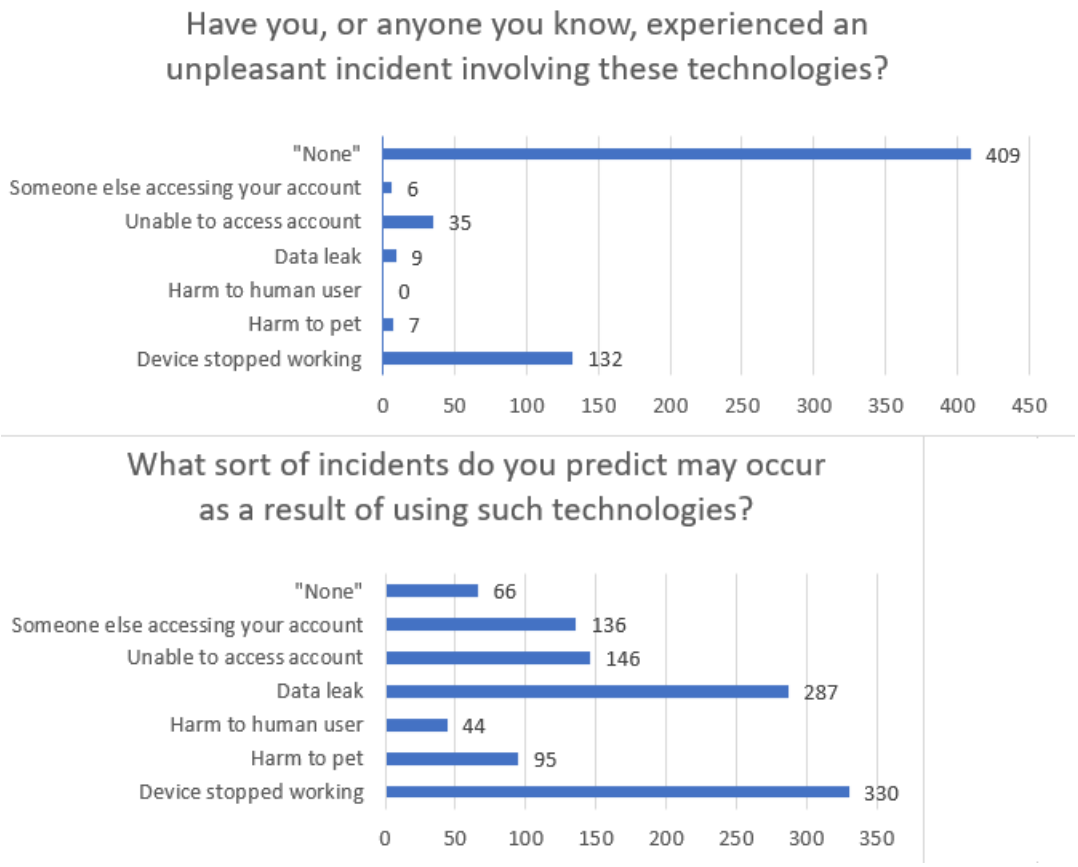

Figure 5.2: The incidents that have occurred to participants and those they predict may occur. x axis is the number of participants

much shared info" and the *"Leak of data"*. Location data was specifically mentioned by some 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"*, showing concerns that these technologies are moving the owners away from their animals, negatively affecting the experiences of the pet and their owners.

5.4.2 Incidents and Attacks

Experiences of Unpleasant Incidents:

For the incidents that have occurred to the participants within the study, they chose "Device stopped working" the most, with 132 participants selecting this option.

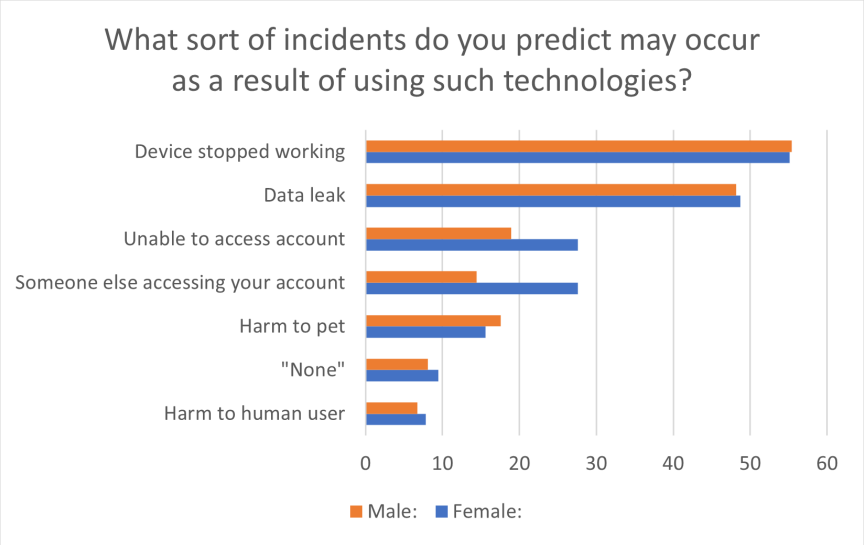

Figure 5.3: Gender comparison of the incidents participants believe may occur.

"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 that were not "none" or equivalent. These responses tell of 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 because of the use of these devices. 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"*. The reported issues vary in type and consequence. As reported, these devices have created a wide range of unpleasant incidents including putting the life of the animal (and potentially human users) at serious risk.

Predicted Incidents:

For incidents that the participants predict may occur, "Device stopped working" was, again, the most selected option, chosen by 330 participants. "Data leak", "Unable to access account", "Someone else accessing your account", "Harm to pet", and finally "Harm to human user" were selected 287, 146, 136, 95, 44 respectively, as can

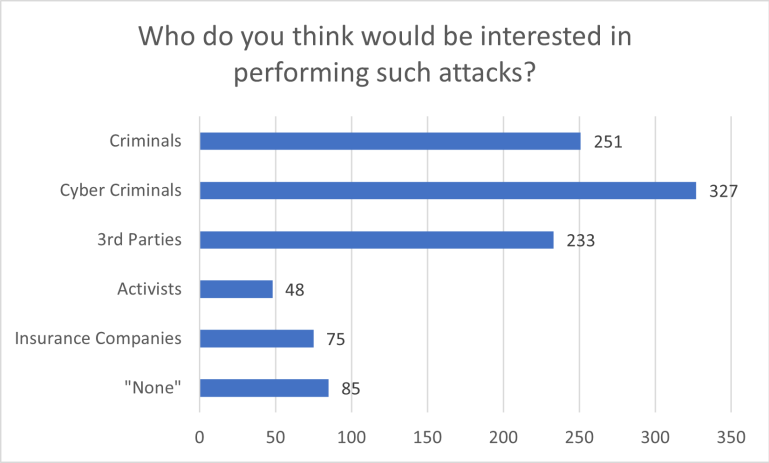

Figure 5.4: Participants report on the potential attackers of pet technologies. x axis is the number of participants.

be seen in Figure 5.3. 72 participants responded with "none" or equivalent. Outside of the available options, multiple participants responded with the possibility of *"over or underfeeding"*. There were also multiple concerns over devices no longer working correctly and *"becoming inaccurate"*. 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.

5.4.3 Potential Attackers

For whom they believed would be responsible for any possible attacks on these pet systems, participants selected the option "Cyber criminals" the most, selected by 327 participants. This was followed by "Criminals", "3rd 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 USA 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

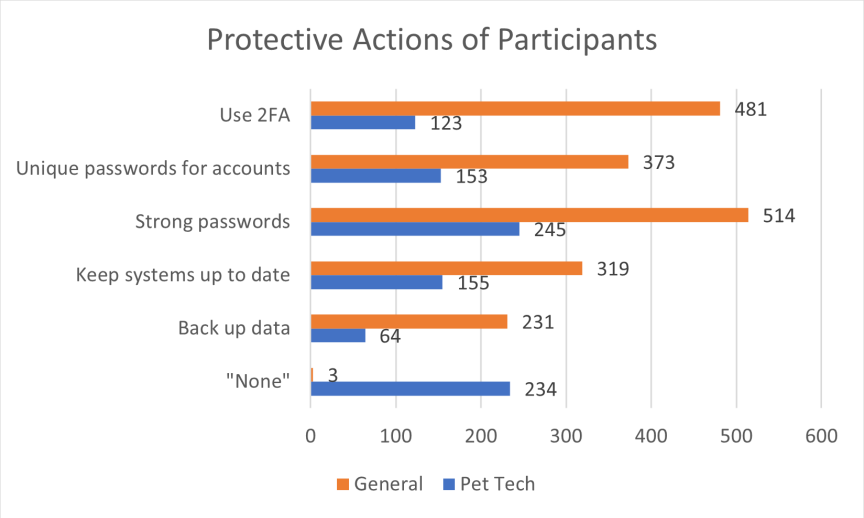

Figure 5.5: Protective actions reported by the participants for general security and privacy vs. pet tech. x axis is the number of participants.

directions, e.g., in the context of intimate partner violence [17, 35].

5.4.4 Protective Actions

At this stage of the survey, we asked our participants about the methods they use to protect their online security in general and animal tech in particular. Here, we present our results.

General Online Security and Privacy Protection: When choosing between the methods they use to protect their general online security and privacy, "Strong passwords" was the most selected option, being chosen 514 times. This was 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 5.5. Only 3 of the participants responded with "none" or equivalent. An additional 3 options were given when asking about general protective actions, these 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 security and privacy. 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 of the participants, adding an extra layer of

security on top of one of the most popular options.

Pet Tech Protective Methods: For protecting the security and privacy 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"*.

As you can see, there are some similarities in the patterns of the responses for protective methods for general security and privacy vs. pet technologies. For instance, in both cases, "Strong passwords" are the most popular method. There are also visible differences across these two categories. For example, not doing anything seems to be the approach that more than a third of our participants reported in response to the pet tech question, while it was chosen by only three participants for the general online protection question.

Desired Protective Measures: When asked what protection measure they would like to be included within their pet technologies, a large number of different options and themes were identified, with variations on multi-factored authentication being by far the most common, mentioned by 122 participants. Different forms of PETs, or privacy enhancing technologies, such as strong security, encryption, biometrics, and vague mentions of stronger security were also mentioned by 122 participants. Passwords and following GDPR practices were the next most mentioned themes, being mentioned by 103 and 70 participants. The rest of the identified themes are; greater user control (32), Not sharing data with 3rd 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 the regulations, e.g., *"As long as they follow data protection protocol"*. It also covers transparency around the data and what is done with it and the security of these systems and if an attack has taken place, 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 security and privacy of these systems. Greater user control covers a variety of

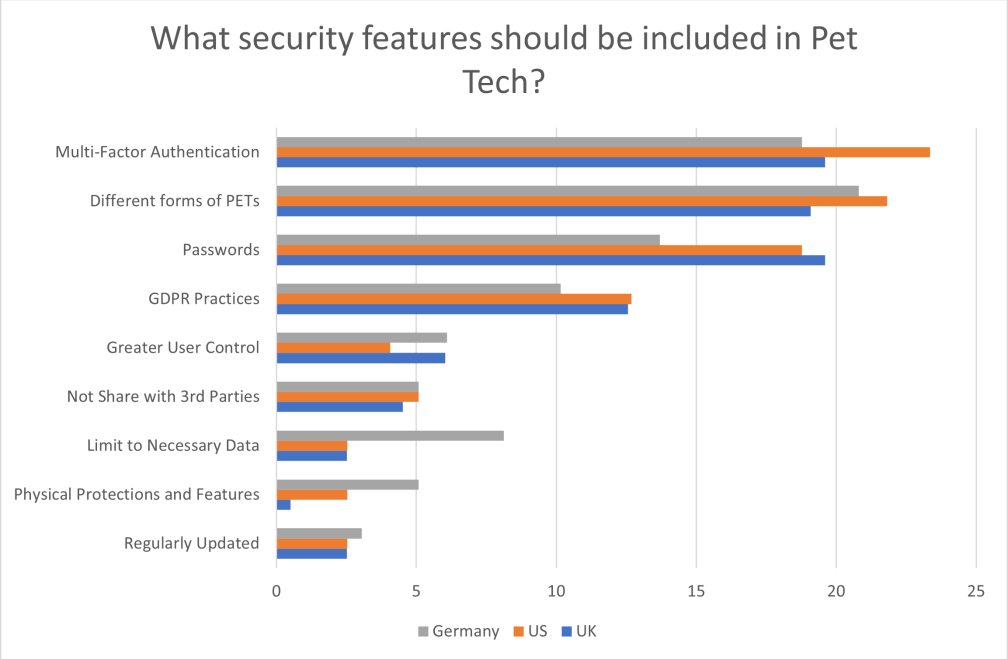

Figure 5.6: The desired protective measures of the participants for pet tech. X-axis is the percentage of participants from each country.

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"*.

Who is Responsible for Pet Tech SP?

When choosing who they believed is responsible for taking care of the security and privacy 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 3rd parties were selected 127, 64, and 38 times respectively.

Few additional responses were given to this question, with multiple participants expressing that they are unsure of who should be responsible. Some additional answers include *"ISP"*, *"Companies hired for security"*, and *"Apple"*, possibly indicating the company in control of the relevant app stores where pet-related apps may be downloaded.

Participants' Additional Comments

We finally asked if the participants had any additional comments about pet technologies. Their responses included General Positive comments about pet technologies (24), security and privacy 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).

5.5 Discussion

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

5.5.1 Security and Privacy Concerns

The participants of this study were found to use a variety of pet technologies, not just microchips. A significant proportion of participants use trackers, cameras, automatic feeders, and automatic water fountains to aid in the care of their pets. Hence, the reported privacy and security issues are in relation to the use of a wide range of pet technologies.

As briefly discussed before, although not many participants have experienced an unpleasant incident whilst using their pet tech, aside from issues with them working, a large number showed concerns over possible future incidents, as reported in Figure 5.2. 287 participants felt that some form of data leak may occur, which would leave their personal information exposed. Another 136 stated that they believed someone may try and access their account, again showing concern about an attacker gaining access to their data. Whilst fewer participants believed their pet or a human user would be put in danger, 95 participants still expressed concern here that their pet may be endangered. These results show that the users mostly believe that their data would be the target, but that pets may also be attacked.

For protecting their data, there is a clear difference between the number of precautions taken for general online use and pet technologies. Far fewer participants selected precaution options when relating to pet technologies as can be seen in Figure 5.5. This highlights that users likely take the risks of pet tech devices and systems less seriously and view attacks against them as less of a threat. This is despite the fact that our findings highlight a belief that a range of attacks may indeed occur when using these technologies.

5.5.2 Comparison to Related Work

We find similar results to that of [131], the study of dog activity monitor users' concerns surrounding a hypothetical data breach. Both our study and this work highlight a lack of concern amongst users with regard to the animal-based data collected. Our results show that pet tech users take fewer precautions compared to their general online security and security. Our participants showed more concern regarding potential data breaches, with just under half of them believing this may occur. Similar to [131], our results show a greater concern for the users' pet's safety than their own, the participants perceive risks to be more likely to their pets than themselves, with double the number of responses predicting harm may come to their pet, as opposed to the user. The most selected possible incident is that the pet's device will stop working. As mentioned before, while harm to the user was not mentioned by our participants commonly, there is research exploring those possibilities, e.g., in the context of intimate partner violence [17, 35]. Similar research in other emerging technologies such as female-oriented technologies (FemTech) shows that the data collected by these connected devices is of interest to multiple threat actors including (ex-)partner and family members and can be misused to harm the users [6, 67, 63].

Our participants showed less concern towards the security of their pet tech devices, compared to their general online security, taking fewer precautions. One possible reason for this is a lack of awareness of the potential risks surrounding the data captured by these devices. Similar gaps in knowledge have been seen in studies of other smart technologies in relation to pet tech. An example is the technologies and sensors used in smart homes and buildings, where users are unaware of the potential risks [15, 141, 121, 1, 25, 81, 142, 39, 46, 45, 122]. However, in these cases, the lack of knowledge did not significantly affect the users' levels of concern. This difference may be explained by the thought that the data collected by these devices does not relate to the user, just to their pet, which they view as harmless. These assumptions have been shown to be incorrect by Van der Linden et al. in [132].

5.5.3 Demographic Comparison

Country: In terms of the data collected by these technologies, there were not many major differences between the participants of different countries. However, UK participants were a bit more likely to select most of the options. German participants, on the other hand, were a little less likely to think that human/owner-related data is collected by these systems, as seen in Figure 5.1. There is not much difference between

the countries when looking at the advantages and disadvantages given regarding pet tech. 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 the peace of mind they can give. Few differences were found in the security features requested by participants. German participants, however, were a bit less likely to select features putting the burden on the user of the system and mentioned limiting the necessary data more than the other countries (Figure 5.6). Following this, German participants were more likely to believe that 3rd parties would be responsible for an incident and that the government should have some responsibility in taking care of the security and privacy 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 [19, 65], the authors discuss how participants across three countries (UK, 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.

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 5.3, 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 security and privacy perception and practice. For example, in [19, 65], 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 potential risks that may account for these concerns, including the increased risks of intimate partner violence faced by women [69]. Another possible risk for these female users is the possibility of someone taking revenge towards them via their pet. Multiple past incidents have involved ex-partners using a woman's pet as a means to get revenge [11, 36]. 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 the possibility of 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 security and privacy 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 [64, 70].

5.5.4 Limitations

We screened for pet owners, focusing on those with cats and dogs, given that most pet tech is designed around them. However, 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) [123]. However, Prolific is aware of these biases and works towards minimising their impact on the research [123]. 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.

5.6 Chapter Summary

In this chapter, we have performed a user study of pet owners, gathering information on their perspectives and views regarding pet technologies and the security and privacy concerns they may have. This study was distributed to just under 600 participants across the United Kingdom, United States of America, and Germany (199, 197, and 197 participants respectively).

Our findings show that a range of these technologies are in use in the real world. Although participants largely have not experienced any sort of incident when using these devices, they do express concerns about the possibility of something occurring. The concerns of the participants seem mostly focused towards their pet, which makes

sense given these health and safety concerns are likely the reasons for purchasing such a device. These concerns, however, are not reflected in the precautions they take, using far fewer methods to protect themselves when using these systems, compared to what they do for their general online security and privacy.

Given these findings, and those of our other projects, we are able to reflect on multiple aspects of the animal tech ecosystem. We will look into how the users' concerns reflect the reality that we have observed through our security and privacy analysis, as well how effective and usable security mechanisms may be introduced and their necessity to maintain the protection of real world users.

Chapter 6

Discussion and Conclusion

In this chapter, we discuss our results across the project's chapters, provide recommendations for various stakeholders, and discuss future research directions.

6.1 Summary of Results

The results of our three studies give various insights into the state of animal technology security and privacy. Here we reflect on the results of our studies before we discuss their overall meaning.

Our security and privacy analysis of apps related to these technologies demonstrates a range of flaws present in systems available to everyday users. The security vulnerability found within this work would have left those using the vulnerable apps susceptible to a relatively easy man-in-the-middle attack. An attacker intercepting the communications during the login process of these apps would be able to view the user's login details (both username and password) in plaintext in a http message. This would clearly give the attacker access to the genuine user's account, giving access to account information and possible further attacks via data such as GPS. The apps were also found to not respect the user's privacy, communicating with a range of tracking services. Many of these communications even happened, just from the app being opened, before the user had a chance to interact at all and consent, clearly violating the GDPR. The apps studied also made a poor effort of effectively displaying their privacy policy in a meaningful way to the user, with the majority of the systems not even mentioning this during the account creation process.

Our proposed identification solution offers a way for resource-constrained IoT devices with limited input methods to verify that they are communicating with another genuine device, making use of inbuilt motion sensors. Our experiments with

the Nordic Thingy 52, an older model of IoT prototyping platform, gave us limited results, despite the relatively promising visual similarity between the signals of the tapping events. The Nordic Thingy 53, a later version of the 52, gave us much more promising results, achieving a 3.5% EER with an FAR of 3% and an FRR of 4% when comparing 100 tapping samples. These results show that a tapping-based alternative for resource-constrained IoT devices is realistic and may be implemented to effectively protect real-world users connecting new devices. Our results are largely comparable to those of related motion-based authentication and fingerprinting works, with the possibility of adjusting the threshold to lower the FAR at the expense of the FRR. These results were obtained using relatively simple signal comparison methods, with limited preprocessing necessary. We also experimented with quantisation as a way to further reduce this demand on resources, however, despite maintaining strong visual similarity post quantisation when using high resolutions, the results were incredibly limited, only ever achieving a best EER of 28.89% on 100 tapping samples.

Our user study helped to inform us about the perspectives of cat and dog owners across a range of countries regarding these technologies that can be used on or around them. It gave us a better understanding of the actual technologies being used by these people, finding that a range of technologies were in use, not just the activity monitors and GPS devices, although these were still the most popular. We found that the possible security and privacy issues of these devices were actually seen as a disadvantage, though not as important as the cost. The results reflect a mindset of prioritising the owner's pet's welfare, focusing on this over all possible drawbacks, blinding them to the risks that may be present. We did find that there were actual concerns amongst the participants of an incident occurring with these devices, despite few having experienced one. However, there was a major discrepancy between their precautions taken for their general online security and privacy and those taken for these devices, despite this concern and desire to protect their pets.

6.2 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.

These vulnerabilities within the user authentication show that there is a need for those developing these technologies to pay more attention to their security, particularly at this stage. Protecting the security of users should be a top priority, to ensure their well-being. As demonstrated by our attack, these early stages of connecting to a device, e.g., account creation or login contain information that is vital to protect. One such stage is the identification and authentication step of connecting to an IoT device, which if intercepted, could result in an attacker gaining access to a user's account or feeding the user false information. By impersonating the user, the attacker may be able to receive information meant for the legitimate user, possibly including personal data. Given the limited interaction methods of many IoT devices, such as the wearables used on animals, identification methods, such as our proposed tapping-based method are vital to ensure these systems do not rely on weak security practices.

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. By taking fewer security precautions, these participants may be putting themselves at risk of attack. Given the differences between the precautions they take for pet technologies and general online tech, it is highly likely that those using these technologies take the security of them 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 likely not to be the priority. It is also possible that this disconnect between the concerns and actions of the participants demonstrates a lack of knowledge of how to effectively protect themselves when using pet tech or other IoT devices. Providing the users of these devices with simpler and more accessible ways to handle these systems securely may enable more of these pet owners to adopt more secure practices.

Many of these pet apps collect personal data about the user, necessitating adherence to GDPR and other privacy policies designed to safeguard human data. Notably, research in [132] reveals that many pet applications even gather more data about the human user than their pet. Given that 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. Moreover, 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. Due to 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.

6.3 Recommendations and Future Work

6.3.1 Animal App Recommendations

With non-human-focused devices collecting large amounts of data about the humans interacting with them, the legislation surrounding these types of devices should receive further research and review. Improvements to the legislation are necessary to better protect those that the systems may not be explicitly designed for. We believe that further research into the current practices, as well as, ways to improve the legislation are needed to motivate those designing these technologies. The intersection of the general data protection regulations, mobile and IoT and animal legislation should be critically studied and the gaps should be addressed internationally.

More generally, educating system developers about best security and privacy practices is fundamental for more trustworthy products. Authors in [60] provide a set of recommendations for those working on developing health systems. This set of recommendations focus on aspects such as authentication, access control, and data retention. Most of these recommendations could be tailored to be applied to animal-based systems too. We believe that modern systems where humans are not the focus should be designed to the same standards as those that are focused on people, given that they are the actual users.

As these technologies continue to develop and spread into further markets, their security and privacy practices should be scrutinised. The methods in our first project may be adapted to analyse the apps of other IoT devices, as well as The communications of the actual devices themselves. Security studies may look to utilise pre-existing tools such as Privacy International's Data Interception Environment, whilst privacy studies could further research the exact data being leaked by these apps and devices and who it is being leaked to. Larger lists of IoT devices and Apps across platforms (e.g., iOS and Android) can be studied by other researchers in the future.

This part of our research received international media attention (Feb-Mar 2023) including an article in the Telegraph[1] on how pet-tracking apps may be "secretly

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

snooping on owners", and an interview with the Naked Scientist [2], 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 one part of this project to the user dimensions of this topic by conducting our user study.

6.3.2 IoT Identification Recommendations

The results of our experiments show that there is promise in the use of motion data and a tapping-based process for generating a shared piece of knowledge for the identification of IoT devices during an authentication process. We show that it is possible to compare this piece of shared knowledge between the two tapped devices and accurately predict whether the devices were a part of that tapping event. Future work should look into implementing the data from other motion sensors or other sensors in general to see whether this can lead to even more accurate identification. It should also look to test this system across different device types, with different motion sensor brands, which would increase the real-world usability of the system.

Testing the system with multiple device types may also help to prove the robustness and real-world applicability of such a system and would be a valuable contribution to the research area. The system may also be tested across platforms, i.e., between a mobile phone and an IoT device, providing further use case scenarios in the real world.

Further testing of this and other possible identification and authentication methods are needed to ensure the security of this growing market of devices that offer unique challenges and communication methods. By offering users a simple to use, but effective authentication method, it lowers the chance of user error and may help them to feel more secure in the use of their IoT devices. These forms of alternative security approaches should be explored, making use of the already available technologies present within many IoT devices.

[2] thenakedscientists.com/articles/interviews/peoples-data-hacked-their-pet-apps

6.3.3 User Study Recommendations

Future work could aim to assess the current knowledge of farmers concerning SP, as well as the risks they are concerned with. Dedicated research can be done to further educate the farmers on the security and privacy risks that they should watch out for, similar to [73]. By empowering the farmers in this way, they will better understand any future investments in these technologies and be less likely to fall victim to an attack. The agriculture industry is a critical national infrastructure and is seeing increased implementation of various technologies, similar to pets.

The disparity between general and pet tech security precautions 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 to potential users, as many of the necessary precautions on the user's end can be applied more generally.

Another avenue for future research, would be to expand on the results of our user study could be done to gain further insights into the reasoning of the users' behaviours and reduced security practices. A more hands on approach may be beneficial for this, with more in depth in-person interviews possibly providing the explanations for this contrast in the concerns and the precautions taken by participants. Such studies will particularly be of interest for at-risk groups such as older adults, children, and women for whom technology abuse opportunities may put them at differential risks.

However, it shouldn't necessarily be entirely on the user to protect themselves; as another direction of research, more studies on the regulation, policy, guidelines, and users are required to gain a more accurate picture of the risks and harms of animal technologies. Stronger regulations on the security protocols used to communicate personal user details should be enforced to ensure all current and newly developed pet devices/apps do not put the user at risk. This sentiment was shared by many of our German participants, who felt the Government be more responsible for protecting users and that these apps should be limited to the amount of data that they can collect about the user.

6.4 Conclusion

In this thesis, we have studied a variety of aspects regarding the security and privacy of animal technologies, looking into real vulnerabilities present, possible security solutions utilising the available sensors, and the users' perspectives.

Before starting with these various projects, we first reviewed the existing literature surrounding the security and privacy of animal technologies and other areas of IoT. This made clear the limited amount of research into these devices, particularly regarding their security and how they may be putting their user's at risk. Based off of this research, we identified a range of questions/challenges from which we based our projects, providing novel contributions to the field of IoT security and privacy.

The first project within this thesis looks to identify whether there are security vulnerabilities present within commercially available animal devices, specifically the apps they communicate with. We find a serious security vulnerability, leaving the user's login details exposed within multiple of the applications studied, as well as multiple poor privacy practices. We additionally review the legislation surrounding animal-based data and animal technologies, finding no mentions that may help to protect those humans using these systems.

Our second project focuses on presenting a possible IoT identification system, making use of the motion sensors present in many IoT devices, particularly animal technologies. Able to work without basic interaction methods, e.g., buttons or a screen, this system compares the collected motion data of two devices that are tapped together. This system provides promising results that may be adapted into a fully fledged authentication system that is simple and effective for users.

The third and final project looks into the user's perspective regarding the security and privacy of pet technologies. Building off our previous projects, we wanted a greater understanding of animal owners viewpoints and concerns. We find that many of the participants are concerned about a possible incident occurring, yet despite this, they take far fewer precautions with their pet devices compared to their general online security and privacy.

The results of our studies highlight various issues present within the animal tech-

nology ecosystem, from poor security practices, to the limited protective actions of participants. We additionally cover some of the possible solutions, discussing a possible IoT identification mechanism and showing that efforts can be made to improve these systems by communicating with those that design them.

The datasets generated within the projects of this thesis and the results obtained from our studies will be made available for researchers upon request. These will be available after the publication of these works. This is in accordance with the values of EPSRC [126, 26, 27].

Bibliography

[1] Noura Abdi, Kopo M Ramokapane, and Jose M Such. More than smart speakers: security and privacy perceptions of smart home personal assistants. In *SOUPS*, 2019.

[2] Lawrence Abrams. Jbs paid $11 million to revil ransomware, $22.5m first demanded, June 2021. `https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/` (last accessed 2 August 2021).

[3] Marshall Abrams and Joe Weiss. Malicious control system cyber security attack case study– maroochy water services, australia, 2008. `https://www.mitre.org/sites/default/files/pdf/08_1145.pdf` (last accessed 25 January 2022).

[4] Amber Adams-Progar, Glenn A. Fink, Ely Walker, and Don Llewellyn. Security and privacy issues in the internet of cows. In Houbing Song, Glenn A. Fink, and Sabina Jeschke, editors, *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications*, Wiley - IEEE, chapter 18, pages 375–398. John Wiley & Sons, Hoboken, NJ, 1st. edition, 2017. `https://ieeexplore.ieee.org/document/8068879`.

[5] Mehrdad Aliasgari, Michael Black, and Nikhil Yadav. Security vulnerabilities in mobile health applications. In *2018 IEEE Conference on Application, Information and Network Security (AINS)*, pages 21–26. IEEE, 2018.

[6] Teresa Almeida, Laura Shipp, Maryam Mehrnezhad, and Ehsan Toreini. Bodies like yours: Enquiring data privacy in femtech. In *Adjunct Proceedings of the 2022 Nordic Human-Computer Interaction Conference*, pages 1–5, 2022.

[7] Manish Prateek Amlan Chakrabarti Amitava Choudhury, Arindam Biswas, editor. *Agricultural Informatics*. Wiley-Scrivener, 2021.

[8] Claudio Badii, Pierfrancesco Bellini, Angelo Difino, and Paolo Nesi. Smart city iot platform respecting gdpr privacy and security aspects. *IEEE Access*, 8:23601–23623, 2020.

[9] Lawrence Baker and Richard Green. Cyber security in uk agriculture, 2021. `https://research.nccgroup.com/wp-content/uploads/2020/07/agriculture-whitepaper-final-online.pdf` (last accessed 8 November 2021).

[10] Thomas Banhazi, Erik Vranken, Dries Berckmans, Luc Rooijakkers, and Daniel Berckmans. 4. word of caution for technology providers: practical problems associated with large scale deployment of plf technologies on commercial farms. In *Precision livestock farming applications: Making sense of sensors to support farm management*, pages 2–10. Wageningen Academic Publishers, 2015.

[11] Mark Branagan. Jilted boyfriend took revenge on ex by snapping their kittens' necks and mutilating their remains with a hammer, mar 2015. `https://www.mirror.co.uk/news/uk-news/jilted-boyfriend-took-revenge-ex-5393743` (last accessed 18 July 2023).

[12] Len Calderone. Smart technology in farming, November 2020. `https://www.agritechtomorrow.com/article/2020/11/smart-technology-in-farming/12486` (last accessed 8 June 2021).

[13] Defense Use Case. Analysis of the cyber attack on the ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, 388:1–29, 2016.

[14] Zeina Chapman and Awais Rashid. Food and farming: Do robots dream of sustainable sheep?, 2021. `https://podcasts.google.com/feed/aHR0cHM6Ly9mZWVkcy5idXp6c3Byb3V0LmNvbS8xODQ3MDM0LnJzcw/episode/QnV6enNwcm91dC05MzQ3MjA3?sa=X&ved=0CAQQkfYCahcKEwiQwJucr4v0AhUAAAAAHQAAAAAQCg` (last accessed 22 October 2021).

[15] Chola Chhetri and Vivian Genaro Motti. Eliciting privacy concerns for smart home devices from a user centered perspective. In *International Conference on Information*, pages 91–101. Springer, 2019.

[16] Ke Wan Ching and Manmeet Mahinderjit Singh. Wearable technology devices security and privacy vulnerability analysis. *International Journal of Network Security & Its Applications*, 8(3):19–30, 2016.

[17] Michelle Cleary, Deependra K Thapa, Sancia West, Mark Westman, and Rachel Kornhaber. Animal abuse in the context of adult intimate partner violence: A systematic review. *Aggression and violent behavior*, 61:101676, 2021.

[18] Scott Coltrane. Research on household labor: Modeling and measuring the social embeddedness of routine family work. *Journal of Marriage and family*, 62(4):1208–1233, 2000.

[19] Kovila PL Coopamootoo, Maryam Mehrnezhad, and Ehsan Toreini. " 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 (USENIX Security 22)*, pages 287–304, 2022.

[20] Constantina Costopoulou, Maria Ntaliani, and Sotiris Karetsos. Studying mobile apps for agriculture. *IOSR J. Mob. Comput. Appl*, 3(6):44–49, 2016.

[21] DeLaval. Sales of milking robots up 20 percent, 2021. `https://www.delaval.com/en-gb/learn/news/sales-of-milking-robots-up-20-percent/` (last accessed 25 October 2021).

[22] Digitanimal. Digitanimal home page, 2017. `https://digitanimal.com/?lang=en` (last accessed 25 October 2021).

[23] Saar Drimer, Steven J Murdoch, et al. Keep your enemies close: Distance bounding against smartcard relay attacks. In *USENIX security symposium*, volume 312, 2007.

[24] Onyeka D'Mello, Mathilde Gelin, Fatma Ben Khelil, Rojen Erik Surek, and Huihui Chi. Wearable iot security and privacy: a review from technology and policy perspective. In *Future Network Systems and Security: 4th International Conference, FNSS 2018, Paris, France, July 9–11, 2018, Proceedings 4*, pages 162–177. Springer, 2018.

[25] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an iot world. In *SOUPS*, 2017.

[26] EPSRC. Policy framework on research data. `https://www.ukri.org/who-we-are/epsrc/our-policies-and-standards/policy-framework-on-research-data/`.

[27] EPSRC. Policy framework on research data. `https://www.ukri.org/who-we-are/epsrc/our-policies-and-standards/policy-framework-on-research-data/principles/`.

[28] Esther. exodus et les pisteurs, April 2018. `https://esther.codes/exodus-et-les-pisteurs/` (last accessed 11 May 2021).

[29] EU. Art. 6 gdpr lawfulness of processing, May 2018. `https://gdpr.eu/article-6-how-to-process-personal-data-legally/`.

[30] James P. Farwell and Rafal Rohozinski. Stuxnet and the future of cyber war. *Survival*, 53(1):23–40, 2011. `https://doi.org/10.1080/00396338.2011.555586`.

[31] Fediaf. Facts & figures 2020 european overview, 2021. `https://www.fediaf.org//who-we-are/european-statistics.html` (last accessed 25 October 2021).

[32] Mikhail Fomichev, Flor Álvarez, Daniel Steinmetzer, Paul Gardner-Stephen, and Matthias Hollick. Survey and systematization of secure device pairing. *IEEE Communications Surveys Tutorials*, 20(1):517–550, 2018.

[33] Gea. Half-yearly financial report q1-q2 2021, 2021. `https://www.gea.com/en/binaries/gea-q2-2021-report_tcm11-90941.pdf` (last accessed 25 October 2021).

[34] Saira Ghafur, Soren Kristensen, Kate Honeyford, Guy Martin, Ara Darzi, and Paul Aylin. A retrospective impact analysis of the wannacry cyberattack on the nhs. *NPJ digital medicine*, 2(1):1–7, 2019.

[35] Crystal J Giesbrecht. Animal safekeeping in situations of intimate partner violence: Experiences of human service and animal welfare professionals. *Journal of interpersonal violence*, 37(17-18):NP16931–NP16960, 2022.

[36] Hasani Gittens. Man kills ex-girlfriend's dog, feeds it to her: Cops, sep 2014. `https://www.nbcnews.com/news/us-news/man-kills-ex-girlfriends-dog-feeds-it-her-cops-n202591` (last accessed 18 July 2023).

[37] Daniel Greene and Katie Shilton. Platform privacies: Governance, collaboration, and the different meanings of "privacy" in ios and android development. *new media & society*, 20(4):1640–1657, 2018.

[38] Thomas Groß. Why privacy is all but forgotten. *Proceedings on Privacy Enhancing Technologies*, 2017(4):97–118, 2017.

[39] Nadine Guhr, Oliver Werth, Philip Peter Hermann Blacha, and Michael H Breitner. Privacy concerns in the smart home context. *SN Applied Sciences*, 2(2):1–12, 2020.

[40] Iakovos Gurulian, Konstantinos Markantonakis, Eibe Frank, and Raja Naeem Akram. Good vibrations: artificial ambience-based relay attack detection. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 481–489. IEEE, 2018.

[41] Ilan Halachmi, editor. *Precision livestock farming applications*. wagening enacademic, 2015.

[42] Scott Harper, Maryam Mehrnezhad, and Matthew Leach. 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)*, pages 38–51. IEEE, 2022.

[43] Scott Harper, Maryam Mehrnezhad, and Matthew Leach. Security and privacy concerns of pet tech users. In *Proceedings of the 12th International Conference on the Internet of Things*, pages 155–162, 2022.

[44] Scott Harper, Maryam Mehrnezhad, and Matthew Leach. Security and privacy of pet technologies: actual risks vs user perception. *Frontiers in The Internet of Things*, 2:1281464, 2023.

[45] Scott Harper, Maryam Mehrnezhad, and John Mace. User privacy concerns in commercial smart buildings. *Journal of Computer Security*, (Preprint):1–33, 2022.

[46] Scott Harper, Maryam Mehrnezhad, and John C Mace. User privacy concerns and preferences in smart buildings. In *International Workshop on Socio-Technical Aspects in Security and Trust*, pages 85–106. Springer, 2020.

[47] HerdWatch. The herdwatch story so far: from concept to changing farmers' lives, 2020. `https://herdwatch.co.uk/about/` (last accessed 25 October 2021).

[48] iLivestock. ilivestock home page, 2020. `https://www.ilivestock.co.uk/` (last accessed 25 October 2021).

[49] Sivanarayani M Karunarathne, Neetesh Saxena, and Muhammad Khurram Khan. Security and privacy in iot smart healthcare. *IEEE Internet Computing*, 25(4):37–48, 2021.

[50] Kippy. Comunicato stampa mamacrowd, 2019. `https://www.kippy.eu/uploads/CS_Kippy_Campagna%20Crowdfunding_01_07_2019.pdf` (last accessed 25 October 2021).

[51] Joseph Kiprop. Best countries for animal welfare, 2018. `https://www.worldatlas.com/articles/best-countries-for-animal-welfare.html` (last accessed 22 October 2021).

[52] Loren Kohnfelder and Praerit Garg. The threats to our products, apr 1999. `https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx` (last accessed 5 November 2021).

[53] Konrad Kollnig, Anastasia Shuba, Reuben Binns, Max Van Kleek, and Nigel Shadbolt. Are iphones really better for privacy? comparative study of ios and android apps. *arXiv preprint arXiv:2109.13722*, 2021.

[54] Lucas J Lara and Marcos H Rostagno. Impact of heat stress on poultry production. *Animals*, 3(2):356–369, 2013.

[55] Wei-Han Lee and Ruby B Lee. Multi-sensor authentication to improve smartphone security. In *2015 International conference on information systems security and privacy (ICISSP)*, pages 1–11. IEEE, 2015.

[56] Lely. Lely reports solid growth in 2020, 2021. `https://www.lely.com/press/2021/03/11/lely-reports-solid-growth-2020/` (last accessed 25 October 2021).

[57] Alla Levina, Vladimir Varyukhin, Dmitry Kaplun, Anna Zamansky, and Dirk van der Linden. A case study exploring side-channel attacks on pet wearables. *IAENG International Journal of Computer Science*, 48(4):878–883, 2021.

[58] Stuart Maisner. Covid: Sharp increase reported in abandoned dogs, 2021. `https://www.bbc.co.uk/news/av/uk-england-kent-57286672` (last accessed 14 November 2021).

[59] Diogo Marques, Tiago Guerreiro, Luís Duarte, and Luís Carriço. Under the table: tap authentication for smartphones. In *27th International BCS Human Computer Interaction Conference (HCI 2013)*. BCS Learning & Development, 2013.

[60] Borja Martínez-Pérez, Isabel De La Torre-Díez, and Miguel López-Coronado. Privacy and security in mobile health apps: a review and recommendations. *Journal of medical systems*, 39(1):1–8, 2015.

[61] Rene Mayrhofer and Hans Gellersen. Shake well before use: Intuitive and secure pairing of mobile devices. *IEEE Transactions on Mobile Computing*, 8(6):792–806, 2009.

[62] Maryam Mehrnezhad. A cross-platform evaluation of privacy notices and tracking practices. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 97–106. IEEE, 2020.

[63] Maryam Mehrnezhad and Teresa Almeida. Caring for intimate data in fertility technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2021.

[64] Maryam Mehrnezhad and Teresa Almeida. " 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*, 2023.

[65] Maryam Mehrnezhad, Kovila Coopamootoo, and Ehsan Toreini. How can and would people protect from online tracking? *Proceedings on Privacy Enhancing Technologies*, 1:105–125, 2022.

[66] Maryam Mehrnezhad, Feng Hao, and Siamak F Shahandashti. Tap-tap and pay (ttp): Preventing the mafia attack in nfc payment. In *Security Standardisation Research: Second International Conference, SSR 2015, Tokyo, Japan, December 15-16, 2015, Proceedings 2*, pages 21–39. Springer, 2015.

[67] Maryam Mehrnezhad, Laura Shipp, Teresa Almeida, and Ehsan Toreini. Vision: Too little too late? do the risks of femtech already outweigh the benefits? In *Proceedings of the 2022 European Symposium on Usable Security*, pages 145–150, 2022.

[68] Luciano B Mendes, Nico WM Ogink, Nadège Edouard, Hendrik Jan C Van Dooren, Ilda De Fátima F Tinôco, and Julio Mosquera. Ndir gas sensor for spatial monitoring of carbon dioxide concentrations in naturally ventilated livestock buildings. *Sensors*, 15(5):11239–11257, 2015.

[69] Elizabeth Miller and Brigid McCaw. Intimate partner violence. *New England Journal of Medicine*, 380(9):850–857, 2019.

[70] Diana M. Moniz, Maryam Mehrnezhad, and Teresa Almeida. 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, 2023.

[71] Mozilla. *privacy not included, 2018. `https://foundation.mozilla.org/en/privacynotincluded/categories/pets/` (last accessed 25 October 2022).

[72] Patrick Mutchler, Adam Doupé, John Mitchell, Chris Kruegel, and Giovanni Vigna. A large-scale study of mobile web app security. In *Proceedings of the Mobile Security Technologies Workshop (MoST)*, page 50, 2015.

[73] NCSC. Cyber security for farmers: Practical tips on how to stay safe, December 2020. `https://www.ncsc.gov.uk/files/NCSC_Cyber%20Security%20Guide%20for%20Farmers-%20digital.pdf`.

[74] Suresh Neethirajan. Recent advances in wearable sensors for animal health management. *Sensing and Bio-Sensing Research*, 12:15–29, 2017.

[75] Toan Nguyen and Nasir Memon. Tap-based user authentication for smartwatches. *Computers & Security*, 78:174–186, 2018.

[76] Muath A Obaidat, Suhaib Obeidat, Jennifer Holst, Abdullah Al Hayajneh, and Joseph Brown. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers*, 9(2):44, 2020.

[77] Times of Israel. Cyber attacks again hit israel's water system, shutting agricultural pumps, 2020. https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/ (last accessed 3 March 2022).

[78] Giangiacomo Olivi and Francesco Armaroli. *UK: Smart Farming: The Rise Of Agritech And Its Legal Issues.* Mondaq, January 2019. https://www.mondaq.com/uk/new-technology/770906/smart-farming-the-rise-of-agritech-and-its-legal-issues.

[79] PFMA. Pfma 2021 annual report, 2021. https://pfma-reports.co.uk/ (last accessed 25 October 2021).

[80] Sarah Prange, Emanuel von Zezschwitz, and Florian Alt. Vision: Exploring challenges and opportunities for usable authentication in the smart home. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 154–158. IEEE, 2019.

[81] Aarathi Prasad, Ruben Ruiz, and Timothy Stablein. Understanding parents' concerns with smart device usage in the home. In *International Conference on Human-Computer Interaction*, pages 176–190. Springer, 2019.

[82] Abbas Razaghpanah, Rishab Nithyanand, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Mark Allman, Christian Kreibich, Phillipa Gill, et al. 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)*, 2018.

[83] RCVS. Gdpr - rcvs information and q&as, March 2018. https://www.rcvs.org.uk/document-library/gdpr-rcvs-information-and-qandas/ (last accessed 13 August 2021).

[84] The Government of the United Kingdom. Animal welfare act 2006, 2006. https://www.legislation.gov.uk/ukpga/2006/45/contents (last accessed 15 July 2021).

[85] The Government of the United Kingdom. Welfare of farmed animals (england) regulations 2007, 2007. https://www.legislation.gov.uk/uksi/2007/2078/contents (last accessed 15 July 2021).

[86] Danish Veterinary and Food Administration. Danish animal welfare act, 2013. https://www.foedevarestyrelsen.dk/english/Animal/AnimalWelfare/Pages/default.aspx (last accessed 22 October 2021).

[87] Department for Environment, Food and Rural Affairs. Code of practice for the welfare of cats, 2017. https://assets.publishing.service.gov.

uk/government/uploads/system/uploads/attachment_data/file/697941/pb13332-cop-cats-091204.pdf (last accessed 16 November 2021).

[88] Department for Environment, Food and Rural Affairs. Code of practice for the welfare of dogs, 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/697953/pb13333-cop-dogs-091204.pdf (last accessed 16 November 2021).

[89] Exodus Privacy. Exodus static analysis, August 2018. https://exodus-privacy.eu.org/en/post/exodus_static_analysis/ (last accessed 2 August 2021).

[90] Exodus Privacy. What exodus privacy does, 2020. https://exodus-privacy.eu.org/en/page/what/ (last accessed 3 May 2021).

[91] Federal Assembly of Switzerland. Tierschutzgesetz 2005, 2005. https://www.fedlex.admin.ch/eli/cc/2008/414/de (last accessed 22 October 2021).

[92] Federal Republic of Germany. Animal welfare act, 2006. https://www.animallaw.info/statute/germany-cruelty-german-animal-welfare-act (last accessed 22 October 2021).

[93] Fullwood Packo. About us, 2020. https://fullwoodpacko.com/about-us/ (last accessed 25 October 2021).

[94] Global Animal Law Association. Animal welfare legislation database, 2021. https://www.globalanimallaw.org/database/national/index.html/ (last accessed 22 October 2021).

[95] Global Stats. Mobile & tablet android version market share united kingdom nov 2020 - oct 2021, 2021. https://gs.statcounter.com/android-version-market-share/mobile-tablet/united-kingdom/#monthly-202011-202110 (last accessed 18 February 2022).

[96] Global Stats. Android version market share worldwide jan 2021 - jan 2022, 2022. https://gs.statcounter.com/os-version-market-share/android (last accessed 18 February 2022).

[97] Government of Austria. Federal act on the protection of animals (animal protection act – tschg), 2004. https://www.globalanimallaw.org/downloads/database/national/austria/erv_2004_1_118.pdf (last accessed 22 October 2021).

[98] Government of the Netherlands. Animals act, 2011. https://wetten.overheid.nl/BWBR0030250/2013-01-01 (last accessed 22 October 2021).

[99] Grand View Research. *Pet Wearable Market Size, Share & Trends Analysis Report By Technology (RFID, GPS, Sensors), By Application (Identification & Tracking, Medical Diagnosis & Treatment), By Region, And Segment Forecasts, 2020 - 2027*. Grand View Research, February 2020. https://www.grandviewresearch.com/industry-analysis/pet-wearable-market (last accessed 8 June 2021).

[100] Information commissioner's Office. *ICO's Children's Code will help protect children online*. ICO, September 2020. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/09/ico-s-children-s-code-will-help-protect-children-online/.

[101] Information commissioner's Office. Consent, 2021. 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. (last accessed 27 January 2022).

[102] International Computer Science Institute. The haystack project, October 2017. https://haystack.mobi/ (last accessed 3 May 2021).

[103] Privacy International. How apps on android share data with facebook, December 2018. https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf.

[104] Research and Markets. *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, January 2019. https://www.researchandmarkets.com/research/xfkc78/global_3_7_bn?w=5 (last accessed 8 June 2021).

[105] Smart Agri Hubs. About smartagrihubs connecting the dots in the agri-tech sector, 2020. https://www.smartagrihubs.eu/about (last accessed 22 October 2021).

[106] State of California Department of Justice. California consumer privacy act of 2018, 2018. https://oag.ca.gov/privacy/ccpa/regs (last accessed 18 November 2021).

[107] State of California Department of Justice. California consumer privacy act of 2018 amendments, 2020. https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-add-adm.pdf (last accessed 18 November 2021).

[108] Statista Research Department. Mobile android os market share in the united kingdom (uk) from 2017 to 2021, by version, 2022. https://www.statista.com/statistics/1185416/mobile-android-market-share-version/ (last accessed 14 February 2022).

[109] Swedish Ministry of Trade and Industry RSL. Animal welfare act (2018: 1192), 2018. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/djurskyddslag-20181192_sfs-2018-1192 (last accessed 22 October 2021).

[110] The Government of the United Kingdom. Animal welfare act 2006, 2006. https://www.legislation.gov.uk/ukpga/2006/45/contents (last accessed 1 November 2021).

[111] The Government of the United Kingdom. Pet theft taskforce policy paper, sep 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014947/Pet_Theft_Taskforce_Report_GOV.UK_PDF.pdf (last accessed 21 October 2021).

[112] The World Organisation for Animal Health (OIE). Terrestrial animal health code (2021), 2021. https://www.oie.int/en/what-we-do/standards/codes-and-manuals/terrestrial-code-online-access/ (last accessed 22 October 2021).

[113] UK Veterinary Medicines Directorate. Record keeping requirements for veterinary medicines, 2013. https://www.gov.uk/guidance/record-keeping-requirements-for-veterinary-medicines (last accessed 14 November 2021).

[114] World Animal Protection. Animal protection index, 2021. https://api.worldanimalprotection.org/ (last accessed 22 October 2021).

[115] Jingjing Ren, Daniel J Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach. In *Proceedings of the Internet Measurement Conference*, pages 267–279, 2019.

[116] Himadri Nath Saha, Reek Roy, Monojit Chakraborty, and Chiranmay Sarkar. Iot-enabled agricultural system application, challenges and security issues. In Amitava Choudhury, Arindam Biswas, Manish Prateek, and Amlan Chakrabarti, editors, *Agricultural Informatics: automation using IoT and machine learning*, Advances in learning analytics for intelligent cloud-IoT systems, chapter 11, pages 223–247. Wiley-

Scrivener, Beverly, MA, 1st. edition, March 2021. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119769231.ch11.

[117] Roy Sahadev, Mukherjee Kaushal, and Arindam Biswas. Plane region step farming, animal and pest attack control using internet of things. In Amitava Choudhury, Arindam Biswas, Manish Prateek, and Amlan Chakrabarti, editors, *Agricultural Informatics: automation using IoT and machine learning*, Advances in learning analytics for intelligent cloud-IoT systems, chapter 12, pages 249–269. Wiley-Scrivener, Beverly, MA, 1st. edition, March 2021. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119769231.ch12.

[118] smaXtec. Smaxtec 2020 round-up, 2021. https://smaxtec.com/en/blog/smaxtec-2020-round-up/ (last accessed 25 October 2021).

[119] Sina Sontowski, Maanak Gupta, Sai Sree Laya Chukkapalli, Mahmoud Abdelsalam, Sudip Mittal, Anupam Joshi, and Ravi Sandhu. Cyber attacks on smart farming infrastructure. In *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*, pages 135–143, 2020.

[120] Anna H Stygar, Yaneth Gómez, Greta V Berteselli, Emanuela Dalla Costa, Elisabetta Canali, Jarkko K Niemi, Pol Llonch, and Matti Pastell. A systematic review on commercially available and validated sensor technologies for welfare assessment of dairy cattle. *Frontiers in Veterinary Science*, 8:177, 2021.

[121] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. " 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)*, pages 435–450, 2019.

[122] Rawan Taher, Maryam Mehrnezhad, and Charles Morisset. "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*, pages 85–106. Springer, 2020.

[123] Prolific Team. What are the advantages and limitations of an online sample?, 2022. https://researcher-help.prolific.co/hc/en-gb/articles/360009501473-What-are-the-advantages-and-limitations-of-an-online-sample-h (last accessed 11 July 2022).

[124] Joe Tidy. Hacker tries to poison water supply of florida city, 2021. https://www.bbc.co.uk/news/world-us-canada-55989843 (last accessed 3 March 2022).

[125] Tracy Turner and Debbie Niemeier. Travel to work and household responsibility: new evidence. *Transportation*, 24:397–419, 1997.

[126] UKRI. Publishing your research findings. `https://www.ukri.org/manage-your-award/publishing-your-research-findings/making-your-research-data-open/`.

[127] Junia Valente, Matthew A Wynn, and Alvaro A Cardenas. Stealing, spying, and abusing: Consequences of attacks on internet of things devices. *IEEE Security & Privacy*, 17(5):10–21, 2019.

[128] Narseo Vallina-Rodriguez, Srikanth Sundaresan, Abbas Razaghpanah, Rishab Nithyanand, Mark Allman, Christian Kreibich, and Phillipa Gill. Tracking the trackers: Towards understanding the mobile advertising and tracking ecosystem. *arXiv preprint arXiv:1609.07190*, 2016.

[129] Dirk van der Linden, Matthew Edwards, Irit Hadar, and Anna Zamansky. Pets without pets: on pet owners' under-estimation of privacy concerns in pet wearables. *Proc. Priv. Enhancing Technol.*, 2020(1):143–164, 2020.

[130] Dirk Van Der Linden, Ola Aleksandra Michalec, and Anna Zamansky. Cybersecurity for smart farming: socio-cultural context matters. *IEEE Technology and Society Magazine*, 39(4):28–35, 2020.

[131] Dirk van der Linden, Emma Williams, Irit Hadar, and Anna Zamansky. Some might freak out: What if your dog's activity tracker were to have a data breach? ACI'19, New York, NY, USA, 2019. Association for Computing Machinery. `https://doi.org/10.1145/3371049.3371057`.

[132] Dirk Van Der Linden, Anna Zamansky, Irit Hadar, Barnaby Craggs, and Awais Rashid. Buddy's wearable is not your buddy: Privacy implications of pet wearables. *IEEE Security & Privacy*, 17(3):28–39, 2019.

[133] Mrinal Wadhwa. A beginners guide to the stride security threat model, 2019. `https://www.ockam.io/learn/blog/introduction_to_STRIDE_security_model` (last accessed 3 November 2021).

[134] He Wang, Dimitrios Lymberopoulos, and Jie Liu. Sensor-based user authentication. In *Wireless Sensor Networks: 12th European Conference, EWSN 2015, Porto, Portugal, February 9-11, 2015. Proceedings 12*, pages 168–185. Springer, 2015.

[135] Hu. Wenjun. Sanddroid. `http://sanddroid.xjtu.edu.cn/` (last accessed 11 April 2022).

[136] Ben Wolford. What are the gdpr consent requirements?, January 2019. `https://gdpr.eu/gdpr-consent-requirements/` (last accessed 10 June 2021).

[137] Matthew Wynn, Kyle Tillotson, Ryan Kao, Andrea Calderon, Andres Murillo, Javier Camargo, Rafael Mantilla, Brahian Rangel, Alvaro A. Cardenas, and Sandra Rueda. Sexual intimacy in the age of smart devices: Are we practicing safe iot? In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, IoTS&P '17, page 25–30, New York, NY, USA, 2017. Association for Computing Machinery. `https://doi.org/10.1145/3139937.3139942`.

[138] Xuanxia Yao, Fadi Farha, Rongyang Li, Ismini Psychoula, Liming Chen, and Huansheng Ning. Security and privacy issues of physical objects in the iot: Challenges and opportunities. *Digital Communications and Networks*, 7(3):373–384, 2021.

[139] Tean Zaheer. Heat stress in animals: Causes, treatment and prevention, 2019. `https://en.engormix.com/poultry-industry/articles/heat-stress-animals-causes-t43940.htm` (last accessed 3 November 2021).

[140] Almos Zarandy, Ilia Shumailov, and Ross Anderson. Hey alexa what did i just type? decoding smartphone sounds with a voice assistant. *arXiv preprint arXiv:2012.00687*, 2020.

[141] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *SOUPS*, pages 65–80, 2017.

[142] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home iot privacy. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):1–20, 2018.

Appendix

A.1 Full Survey

Introduction Text
Hi,
In this survey, we are studying the use of pet technologies and would like to invite you to participate by answering a few questions. Pet technologies refers to devices used on/for pets and includes wearable activity and location monitors, automatic feeders, microchips, and pet health apps, etc.

This study is for UK participants, and participation is completely voluntary and is open to everyone to participate. Our data collection is anonymous and none of your personal data (such as name) will be collected. The questionnaire results are only used for research purposes in this specific study.

This study is conducted by Scott Harper (PhD student), Dr Maryam Mehrnezhad, and Dr Matthew Leach (Newcastle University). If you have any questions or comments, please contact us at:
s.harper@ncl.ac.uk, maryam.mehrnezhad@ncl.ac.uk, and matthew.leach@newcastle.ac.uk

Consent
If you give your consent to take part please click 'I agree' below.

- I agree
- I do not agree

Prolific ID
Please enter your Prolific ID
Open Text

Screener Validation
Do you own a pet?

- Yes
- No

Main Questions

1. What is your Gender?
    - Female
    - Male
    - Non-binary
    - Prefer not to say
2. What is your Age?
   Open Text
3. What is your Occupation?
   Open Text
4. In your own words, please describe what pet technologies are and what they do?
   Open Text
5. What forms of pet technologies do you use? Please name the technology and its application. e.g., GPS tracker, animal health app, and automatic feeder
   Open Text
6. Why do you use these technologies? Please explain
   Open Text
7. What animals do you use pet technologies on/for? Please explain the application of the technology for each animal.
   Open Text
8. How long have you been using these technologies?
   Open Text
9. What types of data (about yourself and your animal) are collected by these technologies? Please explain.
   Open Text
10. What types of data (about yourself and your animal) are collected by these technologies? (Multiple choices)
    - Name of Owner

- Photo of owner
- Pet photo
- Age/Gender of Owner
- Address/location of Owner
- Contact info (mobile, email, ads)
- Social media (Facebook, Instagram, Twitter, ...)
- Basic Pet Info (name, age, sex, etc.)
- Pet Technologies used
- Pet Location
- Pet Activity
- Pet Health (weight, diet, illness, medical conditions, etc.)
- Vet info (name, contact info, address, etc.)
- Appointments (vet, grooming, etc.)
- Treatments (medicine, etc.)
- Food info (brand, amount, schedule, etc.)
- Microchip ID
- Payment Information (Cards)
- Other: *Open Text*

11. What are the benefits of using these technologies? Please explain.
    Open Text

12. What are the benefits of using these technologies? (multiple choices)

    - They are cost-effective
    - They are accurate
    - They are easy to use
    - They save time
    - They are secure
    - They improve my pet's welfare
    - They increase my knowledge about my pet
    - Other: *Open Text*

13. What are the disadvantages of using these technologies? Please explain.
    Open Text

14. What are the disadvantages of using these technologies? (multiple choices)

    - They are expensive
    - They are not accurate
    - They are difficult to use
    - They waste time
    - They are not safe
    - They share user information with third parties or sell to them
    - They are bad for my pet's welfare
    - Other: *Open Text*

15. Have you, or anyone you know, experienced an unpleasant incident involving these technologies? Please explain.
    Open Text

16. Have you, or anyone you know, experienced an unpleasant incident involving these technologies? (multiple choices)

    - Device stopped working
    - Harm to pet
    - Harm to human user
    - Data leak
    - Unable to access account
    - Someone else accessing your account
    - Other: *Open Text*

17. Are you aware of any cyber-attack incidents involving these technologies?
    Open Text

18. Who do you believe has access to your data when using these technologies?
    Open Text

19. Who do you believe has access to your data when using these technologies? (multiple choices)

    - Your vet

- Technology provider
- Researchers
- The company making the app/device
- The operating system of mobile/PC (e.g. Apple, Google. Microsoft)
- Third parties such as insurance companies
- Third parties such as advertising companies
- The government
- The public
- Other: *Open Text*

20. What sort of incidents do you predict may occur as a result of using such technologies? Please explain.
    Open Text

21. What sort of incidents do you predict may occur as a result of using such technologies? (multiple choices)

    - Device stop working
    - Harm to pets
    - Harm to human user
    - Data leak
    - Unable to access account
    - Someone else accessing your account
    - Other: *Open Text*

22. Who do you think would be interested in performing such attacks? Please explain.
    Open Text

23. Who do you think would be interested in performing such attacks? (multiple choices)

    - Criminals
    - Cyber criminals
    - Third parties (e.g. for advertising)
    - Activists
    - Insurance companies
    - Other: *Open Text*

24. What do you generally do to protect your online security (e.g., banking, social media, etc.)?
    Open Text

25. What do you generally do to protect your online security (e.g., banking, social media, etc.)? (multiple choices)

    - Use two-factor authentication
    - Unique passwords for each account
    - Strong passwords
    - Keep systems up to date
    - Back up your data
    - Use a password manager
    - Avoid emails from unknown sources
    - Avoid clicking on unfamiliar links
    - Other: *Open Text*

26. What do you do to protect the security of your pet technology systems?
    Open Text

27. What do you do to protect the security of your pet technology systems? (multiple choices)

    - Use two-factor authentication
    - Unique passwords for each account
    - Strong passwords
    - Keep systems up to date
    - Back up your data
    - Other: *Open Text*

28. Who do you think is responsible for taking care of security and privacy of such systems including the data ownership issues?
    Open Text

29. Who do you think is responsible for taking care of security and privacy of such systems including the data ownership issues? (multiple choices)

    - Owner of the system

- Others that use the systems
- Company that designs the system
- Third parties (e.g., for advertising)
- Government
- Other: *Open Text*

30. What security features should be included in pet technology systems to help you use them without fear of an incident occurring?
    Open Text

31. If you have any other comments about pet technologies, please write them here.
    Open Text

A.2 MATLAB Code

A.2.1 Parallelised EER Calculation - including functions called

```
PeakList1 = { *Device 1: samples 1-100};
PeakList2 = { *Device 2: samples 1-100};


-------------------------------------------
bestNonQuant=55555555;
len = numel(PeakList1);
rangeLen = length(rangeVals); %rangeVals contains all possible weights for a,b,c
maxCoh = 0;
maxEng = 0;

matchingValueList = zeros(rangeLen, len, 6);
nonMatchingValueList = zeros(rangeLen, ((len^2) - len), 6);

% Precompute the matrices outside the parfor loop
tab1List = cell(len, 1);
tab2List = cell(len, 1);

for i = 1:len
    tab1List{i} = PeakList1{i};
    tab2List{i} = PeakList2{i};
end

parfor val = 1:rangeLen
    rangeValsLocal = rangeVals;
    a = rangeValsLocal(val, 1);
    b = rangeValsLocal(val, 2);
    c = rangeValsLocal(val, 3);

    localMatchingList = zeros(len, 6);
    localNonMatchingList = zeros((len^2) - len, 6);
    localCounter = 1;

    % Create local slices of tab1List and tab2List
    localTab1List = tab1List;
    localTab2List = tab2List;

    localMaxCoh = 0;
    localMaxEng = 0;

    for i = 1:len
        tab1 = localTab1List{i};
        for j = 1:len
            tab2 = localTab2List{j};
            [cor, coh, eng] = GraphCompSplit(tab1, tab2);
            tempArray = [cor, coh, eng, a, b, c]; % Local variable
```

```
            if i == j
                localMatchingList(i, :) = tempArray;
            else
                localNonMatchingList(localCounter, :) = tempArray;
                localCounter = localCounter + 1;
            end

            if coh > localMaxCoh
                localMaxCoh = coh;
            end
            if eng > localMaxEng
                localMaxEng = eng;
            end
        end
    end

    matchingValueList(val, :, :) = localMatchingList;
    nonMatchingValueList(val, :, :) = localNonMatchingList;

    % Update global max values
    maxCoh = max(maxCoh, localMaxCoh);
    maxEng = max(maxEng, localMaxEng);
end

disp("1st step done");

setMatchingList = zeros(rangeLen, len);
parfor x = 1:rangeLen
    for y = 1:len
        vals = matchingValueList(x, y, :);
        cor = vals(1);
        coh = vals(2);
        eng = vals(3);
        a = vals(4);
        b = vals(5);
        c = vals(6);
        setMatchingList(x, y) = GraphComp(cor, coh, eng, maxCoh, maxEng, a, b, c);
    end
end
disp("2nd step done");

nmLength = ((len^2) - len);
setNonMatchingList = zeros(rangeLen, (len^2) - len);
parfor x = 1:rangeLen
    for y = 1:nmLength
        vals = nonMatchingValueList(x, y, :);
        cor = vals(1);
        coh = vals(2);
        eng = vals(3);
        a = vals(4);
        b = vals(5);
        c = vals(6);
        setNonMatchingList(x, y) = GraphComp(cor, coh, eng, maxCoh, maxEng, a, b, c);
    end
end
```

```
disp("3rd step done");

% Run Threshold Tests
resultList = zeros(length(rangeVals)*1000,5);
counter=1;
for threshold = 0:+0.001:1
    for countRow = 1:+1:length(rangeVals)
        [eer,far,frr] = errorCheck(setMatchingList(countRow,:),setNonMatchingList(countRow,:),threshold);
        resultList(counter,1) =  eer;
        resultList(counter,2) =  far;
        resultList(counter,3) =  frr;
        resultList(counter,4) =  threshold;
        resultList(counter,5) =  countRow;
        counter = counter +1 ;

        if(eer < bestNonQuant)
            bestNonQuant=eer;
            bestfar = far;
            bestfrr=frr;
            bestthresh=threshold;
            bestres=rangeVals(countRow,:);
        end
    end
end
disp("all done");


    ------------------------------------------


%FAR, FRR, and EER Calculation
function [eer,far,frr] = errorCheck(matching,nonMatching,thresh)
    countFR=1;
    reject=0;
    while countFR <= length(matching) %Calc false rejections
        if matching(countFR) < thresh
            reject = reject + 1;
        end
        countFR=countFR+1;
    end

    countFA=1;
    accept=0;
    while countFA <= length(nonMatching) %Calc false accepts
    %     disp(list2(countFA));
        if nonMatching(countFA) >= thresh
            accept = accept + 1;
        end
        countFA=countFA+1;
    end


    far = accept/length(nonMatching);
    frr = reject/length(matching);
    eer = (far + frr)/2;
```

```
end


    ------------------------------------------


%Generate Correlation Coefficient, Coherence, and Energy Difference for each comparison
function [correlation,coherence,energyDiff] = GraphCompSplit(tab1,tab2)

% Get dydx
dydx1 = diff(tab1(:));
dydx2 = diff(tab2(:));
tab1 = dydx1;
tab2 = dydx2;

% CORRELATION COEFFICIENT
    [R,P] = corrcoef(tab1,tab2);
    correlation =(R(1,2));

% COHERENCE
    cxy = mscohere(tab1,tab2);
    [coherence,n] = sumsqr(cxy);

%   ENERGY OF THE SIGNALS
    FrameLength = 10;   %Possibly test different values for this???
    movrmsWin = dsp.MovingRMS(FrameLength);

    energyPer1 = movrmsWin(tab1);
    energyTotal1 = sum(energyPer1);

    energyPer2 = movrmsWin(tab2);
    energyTotal2 = sum(energyPer2);

%   ENERGY DIFFERENCE \/
    energyDiff = abs(energyTotal1-energyTotal2);

end

------------------------------------------

%Use the above similarity metrics to calculate the overall Similarity of each comparison
function [similarity] = GraphComp(correlation,coherence,energyDiff,maxCoh,maxEng,a,b,c)

%Normalise these values to be inline w/ correlation values
coherence = coherence/maxCoh;
energyDiff = energyDiff/maxEng;


energyDiff = 1-energyDiff; %Needs inverting (prev. smaller was better)

%Combine values, incorporating weights
similarity = a*correlation + b*coherence + c*energyDiff;

end
```