Are Our Animals Leaking Information About Us? Security and Privacy Evaluation of Animal-related Apps

Scott Harper, Maryam Mehrnezhad, Matthew Leach
Newcastle University
Newcastle upon Tyne, United Kingdom
{s.harper, maryam.mehrnezhad, matthew.leach}@newcastle.ac.uk

***Abstract*—Novel technologies are increasingly being applied to farm and companion animals, and are proving popular with those who keep animals. Although this rapidly growing industry is introducing cybersecurity risks to both animals and their owners, it remains an under-researched field. In this study, we have identified multiple security and privacy vulnerabilities by evaluating 40 popular Android apps for farm and companion animals. We demonstrated that several of these applications are putting their users at risk by exposing their login details. The apps also perform poorly in terms of protecting the users' privacy with over half of the apps communicating with a tracker before the user can consent, violating the General Data Protection Regulation (GDPR). Accordingly, only 4 of the apps explicitly informed the user of their privacy policy and obtain consent. Our findings are important since they highlight the poor privacy practices present in animal-based applications, as well as the easily preventable security vulnerabilities that were reported to the companies responsible.**

***Index Terms*—Animal Technologies Security and Privacy, Agritech Security, Security and Privacy Evaluation, Mobile App Security and Privacy, Data Protection Regulations, User Security, User Privacy**

1. Introduction

An expanding variety of monitoring technologies are being offered for the farm and companion animal industries. They include, but are not limited, to sensor-enabled wearables, tracking technologies, outdoor cameras, environmental sensors, feed/water monitoring, etc. In essence, they all collect, process, retain and broadcast data about the animal and its surroundings.

However, their security and privacy features are lacking in various ways. This 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 [1]. This is regardless of the fact that these systems collect information about their human users too [2].

As the demand for animal technologies increases by end-users, for both farm [12] and companion animals [13], 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 [14], 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 [15] 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 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 [2], [6]. In this paper, 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 re-testing, these apps were found to no longer have this serious vulnerability.

TABLE 1. CYBERSECURITY ATTACK EXAMPLES IN ANIMAL TECHNOLOGIES

Attack type	Farm animal	Companion animal
Spoofing	Attacker uses a farmer's phished login details to gain access to their account [4]	Spoofing pet wearable GPS location [3] for ransom or to aid with theft
Tampering	Manipulating environmental temperature to harm the poultry production [5]	Manipulating the feeding/medicine system to harm pets [6]
Repudiation	Deny altering animal health records [7]	Deny ownership of an abandoned pet [8]
Information Disclosure	Stealing the herd health data to damage finance/reputation [9]	Stealing pet microchip info e.g. address & GPS [10] for spamming/phishing attacks
Denial of Service	Service interruptions on remote access tools [11]	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 [4]	Access to and ability to alter owner and pet details

2. Background and Related Work

In this section, we explain modern animal technologies, the policies, guidelines and regulations around such technologies, as well as the existing and potential risks concerning the animals and their owners via these technologies.

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) [16], electrical grids (Ukraine 2015) [17], water treatment plants (Israel 2020 [18], Florida 2021 [19]), nuclear plants (Iran 2010) [20], and healthcare systems (UK 2017) [21] 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 [22] and is considered by many governments as a critical national infrastructure [14]. The implementation of IoT technologies within this sector will enhance its capabilities through increased efficiency and is being seen as the 4th industrial revolution [23]. However, with the increased use of IoT in this sector, it becomes more vulnerable to attack due to the increased attack surface [6], [24]. One of the major concerns in IoT is the possibility for unsafe mobile interfaces [25] 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[1].

Another especially concerning vulnerability is the possibility of food supplies being tampered with by internet entities [14], 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 [25]. Attacks on the agriculture sector will have a lasting impact on the consumers' trust resulting in significant financial consequences [24]. 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" [6]. Given the importance of this sector, and these possible vulnerabilities, data security is a top priority in IoT-based agricultural systems [25] and is an important area to study.

1. farmwizard.co.uk/

2.1. 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 [13] and pet wearables had a market size valued at USD 1.6 billion in 2019 [26]. Kippy, a pet wearable company whose app is studied in this paper, has more than 17,000 active users and are expecting this to increase to 300,000 by 2023 [27]. Fediaf, the European pet food industry, reported the annual sale of pet accessories in 2020 as being 9.2 million [28]. Given the 2.8% annual growth of the pet food industry in 2020 [28] and the recent increase in pets in countries such as the UK (11% of households acquired a new pet) [29], 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[2], tracking a pet's exercise and when they are active e.g. PitPat[3]. Another type of these devices includes GPS tracking, giving the exact location of the animal at a given time e.g Tractive[4]. These tracking devices can also 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[5]). This is specifically concerning since security and privacy regulations vary across the user groups [30].

Furthermore, these types of technologies are now increasingly being used by the farming industry [12]. Herdwatch, iLivestock, Digitanimal, and Fullwood Packo are used by over 10,000, 5000, 3,800, and 50,000 clients/farms respectively [31]–[34]. 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 [35]. Lely also saw growth last year, with an increase of sales from €606 million to €615 million [36]; along with DeLaval, which saw a 20% increase in the sale of their milking robots [37]. These companies anticipate even more growth in this industry, with Gea expecting a further significant increase

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

for 2021 [35] and smaXtec aiming for 1 million cows being monitored by their systems [38].

Wearable sensors on farm animals can take the guesswork out of stock management [39] and help a farm run more efficiently. The work performed by the authors of [40] is one of the few studies that has looked at farm-based mobile applications. They find that there are a very small number of applications available in relation to the sector's significance, however, suggest that "mobile agriculture apps show significant potential for the modernization of the agriculture sector".

For all these devices, there are corresponding online systems or applications that allow users to view and work with the collected data. There are also animal-based applications that are not connected to these devices, such as apps used to monitor a pet's health.

2.2. Potential Risks

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 or be used by an attacker to exploit the user. Previous work such as [41] 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 [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. 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 [42].

As can be seen in Table 1, 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 [4], a security model designed to help anticipate the different cyberattacks that may be possible against a system, to demonstrate a variety of possible attacks.

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 [43]. In the case of farm animal systems, this could involve an attacker gaining access to a farm's account and then interacting with the system or other users. For a pet wearable or any other wearable device, an attacker may be able to spoof the GPS [3], feeding the user incorrect GPS information to prevent them from locating the tracking device. This would help with animal theft or may be used to gain money from the owner.

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 [5] or causing heat stress [44]. 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 [6].

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 animals 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 this possibility of their herd health data being stolen, with this potentially being used by their competition, or to damage their reputation [9]. For pet technologies, this information could be user address information from their pet's microchip or GPS [10] 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 [11] and may prevent them from spotting an animal with a health condition. 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 increasing commonplace [15].

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 admin privileges has the ability to remove animals from the system and potentially also affect their environment. Admin 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. 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.

The security and privacy of mobile apps is a well-studied area for more general applications (e.g. [45]–[51]). However, little research has been done into the security and privacy of applications when they are designed for use with pets and livestock. This could be due to an even lower concern regarding the privacy of applications used with animals compared to other apps, as found in [10]. In this paper, we aim to address this gap by analysing the security and privacy of these applications. We will investigate how secure the communications performed by these applications are and whether they reveal any sensitive information about the user.

3. 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.

3.1. Approach

We selected the top-ranking animal welfare legislation, as ranked by [52] and [53], for our analysis. The animal welfare legislation that we look at include those from Austria [54], Denmark [55], Germany [56], the Netherlands [57], Sweden [58], Switzerland [59], England and Wales [60], and the OIE (World Organisation for Animal Health) [61]. We also look at the General Data Protection Regulation (GDPR) [62] and California Consumer Privacy Act (CCPA) [63], along with its recent amendments [64] 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.

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. 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 [1]. Furthermore, there is no mention of animal applications, smart technologies, or the data that they collect in the current animal legislation in the UK [65], [66], or the codes of practice for pet owners [67], [68] 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 [58], the mention of RFID in ear tags, and that electronic devices used in facilities should be safe for cattle [61]. 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" [59]. In Austria, pet-related data is removed after a fixed period, 20 and 25 years for dogs and cats respectively [54]. 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 [61], 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" [69] 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 [15].

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.

4. 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.

4.1. 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 [2]. 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 2). 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 2. A selection of pet health apps was also selected to be analysed given the possibility that they may also capture data about their users. These 4 apps were again chosen based on their popularity, but also with the ability to either create or login to an account (17-20 in Table 2).

Farm Apps: Again, where possible, the farming apps were chosen from the device list in [70]. 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 2. For the remaining 5 farming applications, the most popular apps where account creation or login is possible were selected (22-26 in Table 2).

4.2. 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 [71] 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.

4.3. Methods

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

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[6] and SpotBugs [7] are examples of static analysis tools that can be used to analyse programs for errors. Parasoft [8] 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[9], which is explicitly designed for identifying trackers and what permissions are used for apps and has been previously used in [48].

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 [10] 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" [11]. The tool Lumen Privacy Monitor [12] 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 [45]–[48].

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" [13]. 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" [72]. 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[14]. 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 in this paper. Privacy International's data interception environment was designed for [73], 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 [47], [48].

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

6. developer.android.com/studio/write/lint
7. spotbugs.github.io
8. parasoft.com
9. exodus-privacy.eu.org/en/
10. eclipse.org/ide/
11. github.com/AndroidHooker/hooker
12. haystack.mobi/
13. androidtcpdump.com/
14. privacyinternational.org/node/2732

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.

4.4. Tools

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

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" [74]. 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 [75]. Exodus runs dexdump[15] 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 [75].

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 [76]. 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 2.

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.

15. 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 [16] 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.

4.5. 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.

4.6. 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 [77]. 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% [78]. Worldwide, it was more than 50% [79]. 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 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 2) 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 2.

16. mitmproxy.org/

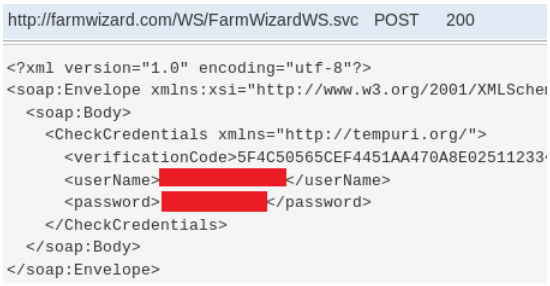

Figure 1. Example of a farming app revealing the user's login details.

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. 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 2) could not be opened whilst the environment was running. The apps would simply not load fully, with the environment reporting that they do not trust the mitmproxy certificate. Another six of the apps (3, 5, 15, 23, 30, 33 in Table 2) 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 2), 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 2) 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.

5. 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.

5.1. Security Vulnerabilities

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

Figure 2. User information displayed in plain text in the HTTP traffic of a Pet app. User details have been anonymised.

5.1.1. 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 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 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.

5.1.2. User info 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 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 2 (Top).

5.2. Privacy Vulnerabilities

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

5.2.1. 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" [80]. 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.

5.2.2. 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. These apps, 1, 25, 29, and 33 in Table 2, 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. This goes against the requirements of the GDPR, which requires consent to be explicitly given by the users [81], 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.

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 2. As stated in article 6 of the GDPR, the processing of user data can only be lawful if the data subject has given consent [82]. 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" [81].

5.3. 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

TABLE 2. TABLE OF PRIVACY RESULTS - THE ANALYSED APPLICATIONS, THEIR FOCUS, NUMBER OF USERS, AND THEIR CORRESPONDING PRIVACY ANALYSIS RESULTS. EXODUS AND LUMEN ANALYSIS RESULTS ARE SHOWN UNDER THEIR RESPECTIVE COLUMNS. X IN LUMEN COLUMN EXPLAINED IN SECTION 3.5. EXPLANATION OF PRIVACY POLICY SYMBOLS CAN BE SEEN IN FIGURE 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

is not surprising given that we did not hear back from its company.

6. 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.

6.1. 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 [10]. 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], [13].

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 [2], many pet applications even collect more data about the human user than their pet.

An attacker with access to the data these devices capture would potentially be able to track the human user,

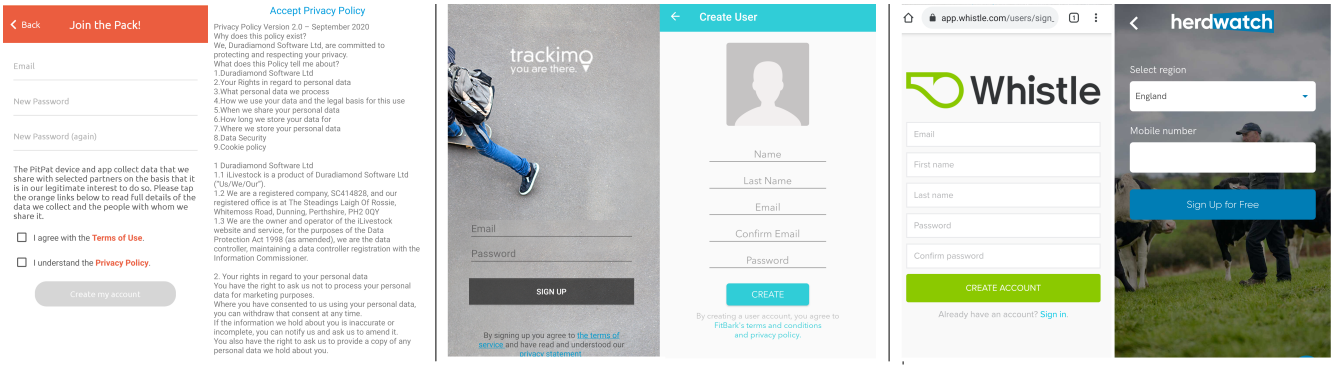

Figure 3. Account creation of 6 apps - Left(✓): PitPat and iLivestock; Middle(-): Trackimo and FitBark; Right(**x**): Whistle and HerdWatch. ✓means that the privacy policy is clearly displayed to the user and that they explicitly have to accept it. – means that although the privacy policy is mentioned, 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.

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 [10] 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.

6.2. 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 [45] (60%) and [46] (75%), analyses of more general apps using Lumen. More of our studied apps have at least five trackers than [45] (20%) and our app set has slightly less than [46] (29%). Like in [73], 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 [47], which looked at the top 116 EU websites and their corresponding apps and, [48], a study on popular Android apps for women's fertility management. In [47], they find that 51% of their apps have no privacy notice and [48] 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, [49] (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 [50], 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, 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 2) 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 2), and the second showing an image of the user's location (6 in table 2). While this is secure against basic traffic interception and observation, it is bad practise 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 [45], [46]. However, they perform better than apps in other studies with more condensed and concentrated app sets such as [47], [48], [73]. 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 [49], [50], 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.

6.3. 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.

With regards 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 [83]. 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 [14], [22] and the rapid growth of these technologies, security and privacy must be considered when designing systems for it. Some recent work such as [6] 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' [84], 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.

6.4. Recommendations

Legislation focusing on data protection and user privacy, such as the GDPR, must take into account newly developing systems, such as those being used on or around animals. Particularly for farms, animal welfare legislation needs to discuss these technologies and the impact they may have on the animals and those around them. Improved legislation will help to protect the data of end-users and lead to the development of more secure and better privacy-preserving products.

More generally, educating system developers about best security and privacy practices is fundamental for more trustworthy products. Authors in [51] 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.

7. Conclusion and Future Work

This paper is the first study to analyse the security as well as the privacy of applications designed for use on or for animals. Our study looks at 40 different applications designed for farm or companion animals. We utilised a range of methods and tools to perform various security assessments including static, dynamic, and network traffic analysis. In addition, we ran a privacy evaluation based on the policies set by data protection regulations. These experiments allowed us to identify these apps' security issues, e.g., with their logins and data transfer. In addition, we observed whether these apps were GDPR-compliant with how they obtain consent from users for tracking services and how they inform the user of their privacy policy and practices.

We found that some of the apps had issues with how they communicate the user's login details, enabling an attacker to intercept the login process and gain the user's login information, as well as some other user details such as the user address. We also found that the apps performed very poorly in terms of user privacy, with more than half of the apps interacting with a tracking service before the user is able to consent. The apps also performed poorly when getting the user to agree to their privacy policy, with only four apps explicitly getting the user to agree to the policy. On top of this analysis, a review of the current top animal welfare and privacy legislation was performed. From this, we find a complete lack of legislation surrounding these increasingly commonplace animal technologies.

Our work shows that greater consideration needs to be taken when designing animal-based applications so that they effectively protect the security and privacy of their human users and the welfare of the animals. We have provided suggestions to improve the regulations surrounding the data these apps collect and store, animal welfare legislation, the practices of those designing these apps and their corresponding devices, and the education of those that use these applications.

Future work could aim to assess the current knowledge level of farmers and pet owners with regards to security and privacy, highlighting gaps in knowledge. For example, dedicated research can be be done to further educate the farmers on the security and privacy risks that they should watch out for, similar to [84]. 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. In addition, studying the security and privacy concerns of animal owners is essential to design the next generation of animal technologies in a more secure way. This will help the end users to improve the quality of their lives and of their animals without experiencing any risk or fear.

8. Acknowledgments

This work was funded by the Engineering and Physical Sciences Research Council (U.K.) through a DTP studentship (EP/T517914/1). We would also like to thank the management of Newcastle University Farms for their help in identifying animal technologies and for helping with access to some of the farm-based apps.

References

[1] RCVS, "Gdpr - rcvs information and q&as," RCVS, Mar. 2018. [Online]. Available: https://www.rcvs.org.uk/document-library/gdpr-rcvs-information-and-qandas/

[2] D. Van Der Linden, A. Zamansky, I. Hadar, B. Craggs, and A. Rashid, "Buddy's wearable is not your buddy: Privacy implications of pet wearables," *IEEE Security & Privacy*, vol. 17, no. 3, pp. 28–39, 2019.

[3] McAfee. (2020) What is gps spoofing? [Online]. Available: https://www.mcafee.com/blogs/internet-security/what-is-gps-spoofing/

[4] L. Kohnfelder and P. Garg, "The threats to our products," apr 1999. [Online]. Available: https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx

[5] L. J. Lara and M. H. Rostagno, "Impact of heat stress on poultry production," *Animals*, vol. 3, no. 2, pp. 356–369, 2013.

[6] L. Baker and R. Green. (2021) Cyber security in uk agriculture. [Online]. Available: https://research.nccgroup.com/wp-content/uploads/2020/07/agriculture-whitepaper-final-online.pdf

[7] UK Veterinary Medicines Directorate. (2013) Record keeping requirements for veterinary medicines. [Online]. Available: https://www.gov.uk/guidance/record-keeping-requirements-for-veterinary-medicines

[8] S. Maisner. (2021) Covid: Sharp increase reported in abandoned dogs. [Online]. Available: https://www.bbc.co.uk/news/av/uk-england-kent-57286672

[9] L. Abrams. (2021, Jun.) Jbs paid $11 million to revil ransomware, $22.5m first demanded. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/

[10] D. van der Linden, M. Edwards, I. Hadar, and A. Zamansky, "Pets without pets: on pet owners' under-estimation of privacy concerns in pet wearables." *Proc. Priv. Enhancing Technol.*, vol. 2020, no. 1, pp. 143–164, 2020.

[11] S. Sontowski, M. Gupta, S. S. Laya Chukkapalli, M. Abdelsalam, S. Mittal, A. Joshi, and R. Sandhu, "Cyber attacks on smart farming infrastructure," in *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*, 2020, pp. 135–143.

[12] L. Calderone. (2020, Nov.) Smart technology in farming. AgriTech Tomorrow. [Online]. Available: https://www.agritechtomorrow.com/article/2020/11/smart-technology-in-farming/12486

[13] 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, Jan. 2019. [Online]. Available: https://www.researchandmarkets.com/research/xfkc78/global_3_7_bn?w=5

[14] A. Adams-Progar, G. A. Fink, E. Walker, and D. Llewellyn, "Security and privacy issues in the internet of cows," in *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications*, 1st ed., ser. Wiley - IEEE, H. Song, G. A. Fink, and S. Jeschke, Eds. Hoboken, NJ: John Wiley & Sons, 2017, ch. 18, pp. 375–398. [Online]. Available: https://ieeexplore.ieee.org/document/8068879

[15] The Government of the United Kingdom, "Pet theft taskforce policy paper," sep 2021. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014947/Pet_Theft_Taskforce_Report_GOV.UK_PDF.pdf

[16] M. Abrams and J. Weiss, "Malicious control system cyber security attack case study– maroochy water services, australia," 2008. [Online]. Available: https://www.mitre.org/sites/default/files/pdf/08_1145.pdf

[17] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.

[18] "Cyber attacks again hit israel's water system, shutting agricultural pumps," 2020. [Online]. Available: https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/

[19] "Hacker tries to poison water supply of florida city," 2021. [Online]. Available: https://www.bbc.co.uk/news/world-us-canada-55989843

[20] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011. [Online]. Available: https://doi.org/10.1080/00396338.2011.555586

[21] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi, and P. Aylin, "A retrospective impact analysis of the wannacry cyberattack on the nhs," *NPJ digital medicine*, vol. 2, no. 1, pp. 1–7, 2019.

[22] R. Sahadev, M. Kaushal, and A. Biswas, "Plane region step farming, animal and pest attack control using internet of things," in *Agricultural Informatics: automation using IoT and machine learning*, 1st ed., ser. Advances in learning analytics for intelligent cloud-IoT systems, A. Choudhury, A. Biswas, M. Prateek, and A. Chakrabarti, Eds. Beverly, MA: Wiley-Scrivener, March 2021, ch. 12, pp. 249–269. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119769231.ch12

[23] Smart Agri Hubs. (2020) About smartagrihubs connecting the dots in the agri-tech sector. [Online]. Available: https://www.smartagrihubs.eu/about

[24] Z. Chapman and A. Rashid, "Food and farming: Do robots dream of sustainable sheep?" 2021. [Online]. Available: https://podcasts.google.com/feed/aHR0cHM6Ly9mZWVkcy5idXp6c3Byb3V0LmNvbS8xODQ3MDM0LnJzcw/episode/QnV6enNwcm91dC05MzQ3MjA3?sa=X&ved=0CAQQkfYCahcKEwiQwJucr4v0AhUAAAAAHQAAAAAQCg

[25] H. N. Saha, R. Roy, M. Chakraborty, and C. Sarkar, "Iot-enabled agricultural system application, challenges and security issues," in *Agricultural Informatics: automation using IoT and machine learning*, 1st ed., ser. Advances in learning analytics for intelligent cloud-IoT systems, A. Choudhury, A. Biswas, M. Prateek, and A. Chakrabarti, Eds. Beverly, MA: Wiley-Scrivener, March 2021, ch. 11, pp. 223–247. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119769231.ch11

[26] 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, Feb. 2020. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/pet-wearable-market

[27] Kippy. (2019) Comunicato stampa mamacrowd. [Online]. Available: https://www.kippy.eu/uploads/CS_Kippy_Campagna%20Crowdfunding_01_07_2019.pdf

[28] Fediaf. (2021) Facts & figures 2020 european overview. [Online]. Available: https://www.fediaf.org//who-we-are/european-statistics.html

[29] PFMA. (2021) Pfma 2021 annual report. [Online]. Available: https://pfma-reports.co.uk/

[30] Information commissioner's Office, *ICO's Children's Code will help protect children online*, ICO, Sep. 2020. [Online]. Available: 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/

[31] HerdWatch. (2020) The herdwatch story so far: from concept to changing farmers' lives. [Online]. Available: https://herdwatch.co.uk/about/

[32] iLivestock. (2020) ilivestock home page. [Online]. Available: https://www.ilivestock.co.uk/

[33] Digitanimal. (2017) Digitanimal home page. [Online]. Available: https://digitanimal.com/?lang=en

[34] Fullwood Packo. (2020) About us. [Online]. Available: https://fullwoodpacko.com/about-us/

[35] Gea. (2021) Half-yearly financial report q1-q2 2021. [Online]. Available: https://www.gea.com/en/binaries/gea-q2-2021-report_tcm11-90941.pdf

[36] Lely. (2021) Lely reports solid growth in 2020. [Online]. Available: https://www.lely.com/press/2021/03/11/lely-reports-solid-growth-2020/

[37] DeLaval. (2021) Sales of milking robots up 20 percent. [Online]. Available: https://www.delaval.com/en-gb/learn/news/sales-of-milking-robots-up-20-percent/

[38] smaXtec. (2021) Smaxtec 2020 round-up. [Online]. Available: https://smaxtec.com/en/blog/smaxtec-2020-round-up/

[39] Allflex. (2020) Allflex sensehub monitoring system. Allflex. [Online]. Available: https://shop.allflex.co.uk/sensehub-by-allflex

[40] C. Costopoulou, M. Ntaliani, and S. Karetsos, "Studying mobile apps for agriculture," *IOSR J. Mob. Comput. Appl*, vol. 3, no. 6, pp. 44–49, 2016.

[41] J. Valente, M. A. Wynn, and A. A. Cardenas, "Stealing, spying, and abusing: Consequences of attacks on internet of things devices," *IEEE Security & Privacy*, vol. 17, no. 5, pp. 10–21, 2019.

[42] S. Prange, E. von Zezschwitz, and F. 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)*. IEEE, 2019, pp. 154–158.

[43] M. Wadhwa. (2019) A beginners guide to the stride security threat model. [Online]. Available: https://www.ockam.io/learn/blog/introduction_to_STRIDE_security_model

[44] T. Zaheer. (2019) Heat stress in animals: Causes, treatment and prevention. [Online]. Available: https://en.engormix.com/poultry-industry/articles/heat-stress-animals-causes-t43940.htm

[45] N. Vallina-Rodriguez, S. Sundaresan, A. Razaghpanah, R. Nithyanand, M. Allman, C. Kreibich, and P. Gill, "Tracking the trackers: Towards understanding the mobile advertising and tracking ecosystem," *arXiv preprint arXiv:1609.07190*, 2016.

[46] A. Razaghpanah, R. Nithyanand, N. Vallina-Rodriguez, S. Sundaresan, M. Allman, C. Kreibich, P. 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.

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

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

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

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

[51] B. Martínez-Pérez, I. De La Torre-Díez, and M. López-Coronado, "Privacy and security in mobile health apps: a review and recommendations," *Journal of medical systems*, vol. 39, no. 1, pp. 1–8, 2015.

[52] World Animal Protection. (2021) Animal protection index. [Online]. Available: https://api.worldanimalprotection.org/

[53] Global Animal Law Association. (2021) Animal welfare legislation database. [Online]. Available: https://www.globalanimallaw.org/database/national/index.html/

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

[55] Danish Veterinary and Food Administration, "Danish animal welfare act," 2013. [Online]. Available: https://www.foedevarestyrelsen.dk/english/Animal/AnimalWelfare/Pages/default.aspx

[56] Federal Republic of Germany, "Animal welfare act," 2006. [Online]. Available: https://www.animallaw.info/statute/germany-cruelty-german-animal-welfare-act

[57] Government of the Netherlands, "Animals act," 2011. [Online]. Available: https://wetten.overheid.nl/BWBR0030250/2013-01-01

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

[59] Federal Assembly of Switzerland, "Tierschutzgesetz 2005," 2005. [Online]. Available: https://www.fedlex.admin.ch/eli/cc/2008/414/de

[60] The Government of the United Kingdom, "Animal welfare act 2006," 2006. [Online]. Available: https://www.legislation.gov.uk/ukpga/2006/45/contents

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

[62] EU, "General data protection regulation (gdpr)," GDPR.eu, May 2018. [Online]. Available: https://gdpr.eu/article-6-how-to-process-personal-data-legally/

[63] State of California Department of Justice, "California consumer privacy act of 2018," 2018. [Online]. Available: https://oag.ca.gov/privacy/ccpa/regs

[64] ——, "California consumer privacy act of 2018 amendments," 2020. [Online]. Available: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-add-adm.pdf

[65] The Government of the United Kingdom, "Animal welfare act 2006," 2006. [Online]. Available: https://www.legislation.gov.uk/ukpga/2006/45/contents

[66] ——, "Welfare of farmed animals (england) regulations 2007," 2007. [Online]. Available: https://www.legislation.gov.uk/uksi/2007/2078/contents

[67] Department for Environment, Food and Rural Affairs, "Code of practice for the welfare of dogs," 2017. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/697953/pb13333-cop-dogs-091204.pdf

[68] ——, "Code of practice for the welfare of cats," 2017. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/697941/pb13332-cop-cats-091204.pdf

[69] J. Kiprop, "Best countries for animal welfare," 2018. [Online]. Available: https://www.worldatlas.com/articles/best-countries-for-animal-welfare.html

[70] A. H. Stygar, Y. Gómez, G. V. Berteselli, E. Dalla Costa, E. Canali, J. K. Niemi, P. Llonch, and M. Pastell, "A systematic review on commercially available and validated sensor technologies for welfare assessment of dairy cattle," *Frontiers in Veterinary Science*, vol. 8, p. 177, 2021.

[71] Information commissioner's Office, "Consent," 2021. [Online]. Available: 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.

[72] H. Wenjun, "Sanddroid," Xi'an Jiaotong University. [Online]. Available: http://sanddroid.xjtu.edu.cn/

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

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

[75] ——. (2018, Aug.) Exodus static analysis. Exodus Privacy. [Online]. Available: https://exodus-privacy.eu.org/en/post/exodus_static_analysis/

[76] International Computer Science Institute. (2017, Oct.) The haystack project. International Computer Science Institute. [Online]. Available: https://haystack.mobi/

[77] Statista Research Department, “Mobile android os market share in the united kingdom (uk) from 2017 to 2021, by version,” 2022. [Online]. Available: https://www.statista.com/statistics/1185416/mobile-android-market-share-version/

[78] Global Stats, “Mobile & tablet android version market share united kingdom nov 2020 - oct 2021,” 2021. [Online]. Available: https://gs.statcounter.com/android-version-market-share/mobile-tablet/united-kingdom/#monthly-202011-202110

[79] ——, “Android version market share worldwide jan 2021 - jan 2022,” 2022. [Online]. Available: https://gs.statcounter.com/os-version-market-share/android

[80] Esther. (2018, Apr.) exodus et les pisteurs. Esther codes. [Online]. Available: https://esther.codes/exodus-et-les-pisteurs/

[81] B. Wolford. (2019, Jan.) What are the gdpr consent requirements? GDPR.eu. [Online]. Available: https://gdpr.eu/gdpr-consent-requirements/

[82] EU, “Art. 6 gdpr lawfulness of processing,” GDPR.eu, May 2018. [Online]. Available: https://gdpr.eu/article-6-how-to-process-personal-data-legally/

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

[84] NCSC, “Cyber security for farmers: Practical tips on how to stay safe,” NCSC, Dec. 2020. [Online]. Available: https://www.ncsc.gov.uk/files/NCSC_Cyber%20Security%20Guide%20for%20Farmers-%20digital.pdf