







Pet technology, meant to provide help and security for pets and owners, has vulnerabilities of its own

January 26 2024, by Stephanie Baum

		
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 night vision.	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

Examples of pet technologies used by the participants of the user study. Credit: *Frontiers in the Internet of Things* (2023). DOI: 10.3389/friot.2023.1281464

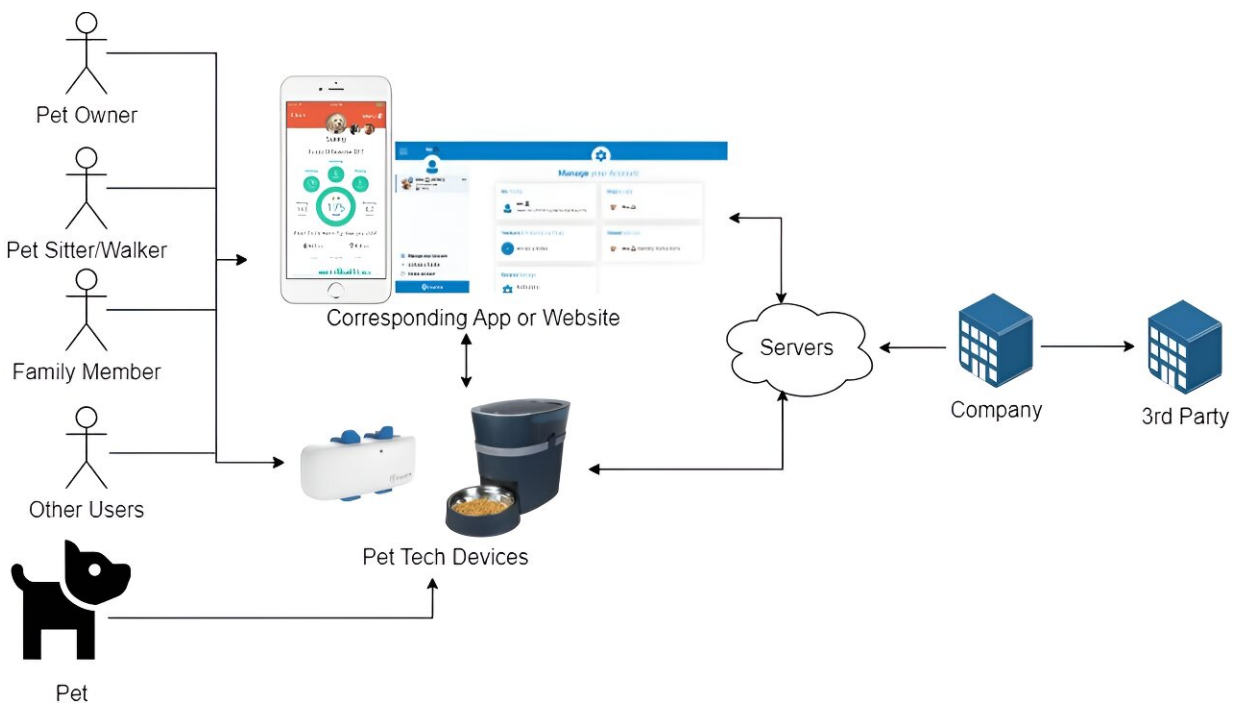
Pet owners are increasingly turning to technology for various pet care purposes such as feeding, health monitoring and activity and movement tracking. Much of this technology operates via devices and apps connected to the Internet of Things (IoT), thereby presenting privacy and

security risks to those who use them.

What are the risks, how serious are they, and what measures have [pet owners](#) taken to protect themselves?

These issues and questions are the topic of a new [study](#) titled "Security and privacy of pet technologies: actual risks vs. user perception" by a research team from the U.K.'s Newcastle University and the University of London. It is published in *Frontiers in the Internet of Things*.

Technologies are available for many aspects of pet care. Owners can use apps and devices to remotely feed their animals; dispense them water and medication; play with them (e.g. automatic ball launchers for dogs); directly watch and listen to them via cameras; and via wearables, monitor their activity and track their movements via GPS.



The pet technology ecosystem; showing how users interact with these systems.

Other users may include vets, insurance companies, health clinics, etc. Arrows represent the flow of data. Credit: *Frontiers in the Internet of Things* (2023). DOI: 10.3389/friot.2023.1281464

However, despite pet tech's projected market value of \$3.7 billion by 2026, only a few studies to date have specifically addressed its privacy and security. That it functions via the IoT implies that in the event of a security breach, an owner's personal information—such as their home address and details on household residents, including pets and children—could be exposed; or that an app or device tasked with a crucial function—such as a medication dispenser—could be misused or simply shut down.

In this new investigation, the researchers first analyzed the privacy and security practices and vulnerabilities of 20 commonly-used pet tech apps, and then surveyed a group of 593 users from Germany, the UK and the US to ascertain which technology they were using; their experiences with its security vulnerabilities; their awareness, needs, and concerns over such; and the measures they had taken to protect themselves and their pets.

The researchers also performed a detailed assessment of legislation from seven European nations, the European Union, and the U.S. state of California addressing [animal welfare](#) and privacy for specific mentions of pet technology with regard to privacy and security. Finally, the team compared the users' perceptions of and concerns about the technology to its actual risks.

Request	Response	Details
POST http://145.239.252.200/WebService/loginver2 HTTP/1.1		
Content-Type	application/x-www-form-urlencoded	
Content-Length	111	
Host	145.239.252.200	
Connection	Keep-Alive	
Accept-Encoding	identity	
User-Agent	okhttp/4.2.1	
<pre>password: [REDACTED] app_version: 1.1.13 device_id: default os_type: android username: [REDACTED]</pre>		

Example of a pet app revealing the user's login details. Login details have been anonymized. Credit: Frontiers in the Internet of Things (2023). DOI: 10.3389/friot.2023.1281464

A lack of regulation and loose technology security

Among the notable findings, the assessment found that in contrast to laws regulating the use of tech to collect and store human-related data, almost no legal regulation exists to set privacy and security standards in the area of pet technology. The team confirmed this through discussion with animal technology experts in both academia and industry.

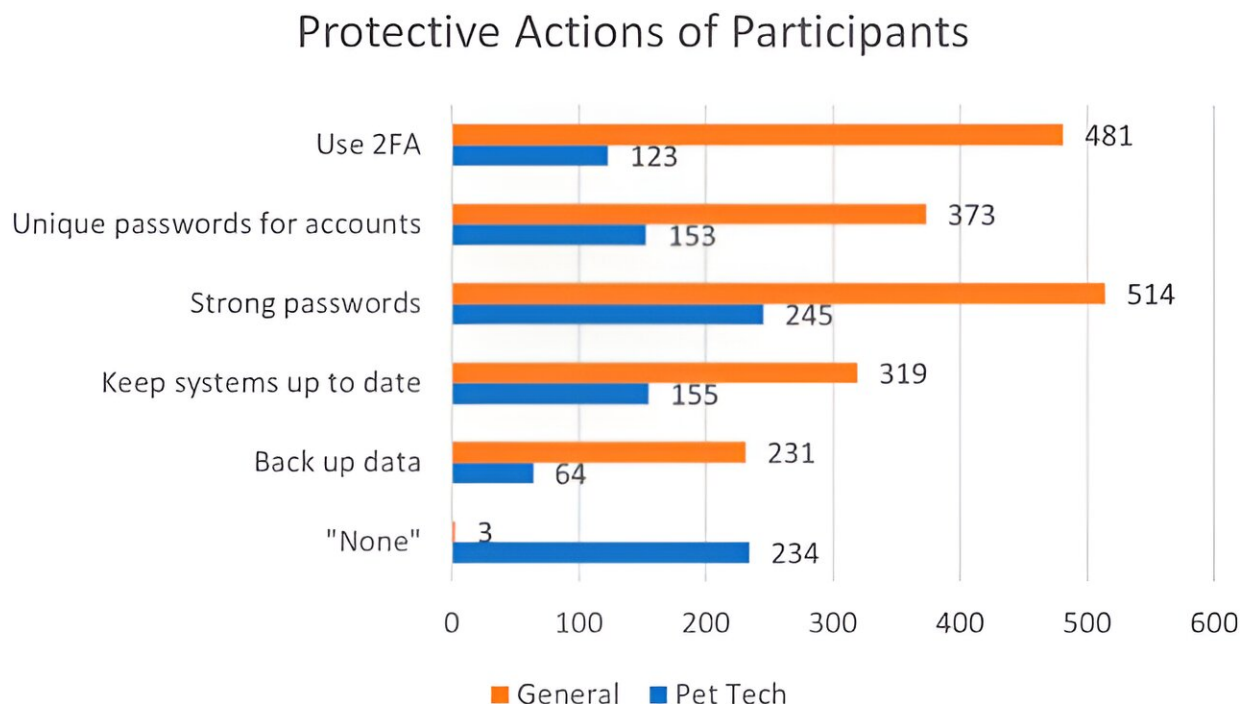
The implications of this gap are profound. The paper states, "Given the lack of regulation, animal applications that do not store any data relating to people do not need to follow the same restrictions as apps designed for humans. However, many of these apps do capture data about people or data relating to the actions of individuals."

In fact, the team found that two of the 20 apps they looked at "had the user's login details visible in plain text within non-secure HTTP traffic," according to the paper. They also found that one of these apps would permit a bad actor to determine the exact location of a user's pet, and that both provided a wealth of detailed information about users (name, address, phone number, email) and their pets (health conditions, medications, and more).

The researchers contacted the companies behind both apps regarding these vulnerabilities. One company subsequently implemented HTTPS encryption for its communications; the other never responded.

Inability to consent to privacy policies

Nineteen of the 20 apps also included at least one form of tracking software, and 14 of these began tracking users before giving them the chance to consent.



Protective actions reported by the participants for general SP vs. pet tech. X-axis is the number of participants. Credit: *Frontiers in the Internet of Things* (2023). DOI: 10.3389/friot.2023.1281464

Regarding privacy, only one of the 20 apps clearly displayed a privacy policy to users and required them to indicate their agreement.

Nine others did not mention or display any privacy policy upon user registration, and the other 10 only provided a link to a privacy policy without displaying it. This violates the EU's 2018 General Data Protection Regulation (GDPR; one of the legislative policies included in the team's assessment), which stipulates that user consent must be given in order for user data to be processed.

Furthermore, the paper states, "None of the apps allow the user to decline the privacy policy and continue to use the app," which also violates the GDPR.

Respondent experiences and predictions

There were 199 participants from the U.K., 197 from the U.S., and 197 from Germany. Of these, 511 confirmed using some form of pet tech; the most common included automatic feeders, cameras, GPS/location trackers, and microchips. Many participants also reported using smart toys and mobile apps for health tracking.

Notably, among commonly reported incidents, there were 132 reports of devices that stopped working and 35 respondents who reported being unable to access their accounts. Nine respondents reported data leaks,

seven reported harm to their pets, and six reported that someone else had accessed their account.

None of the respondents reported specific incidents of harm to a human user, and in fact there were 409 affirmative responses of "none" regarding harm to a human.

But when it came to predictions, more respondents (330) believed that they could experience a device not working than those who speculated that they might encounter a data leak (287), inability to access their account (146), unauthorized account access by someone else (136), or harm to their pet (95) or themselves (44).

Respondent privacy and security precautions

Though relatively few of the survey respondents reported experiencing actual privacy or security incidents, many more of them believed that it could happen. But the researchers noted that significantly fewer respondents reported taking similar security measures specifically with their pet tech than they generally did.

This was true in every case for questions about two-factor authentication, unique account passwords, strong passwords, performing system updates, backing up data, and taking any security precautions as opposed to none.

What is needed next?

The researchers conclude with many recommendations for providing more and improved precautionary information to users of IoT devices and pet tech, stronger regulations on such technology, and privacy and security improvements to the technology itself.

They also call for further research in this field "in the hope of offering practical solutions to improve the quality of the lives of the animals and their owners without any risk and fear of the security, privacy, and safety of both the animals and owners."

More information: Scott Harper et al, Security and privacy of pet technologies: actual risks vs user perception, *Frontiers in the Internet of Things* (2023). [DOI: 10.3389/friot.2023.1281464](https://doi.org/10.3389/friot.2023.1281464)

© 2024 Science X Network

Citation: Pet technology, meant to provide help and security for pets and owners, has vulnerabilities of its own (2024, January 26) retrieved 9 May 2024 from <https://techxplore.com/news/2024-01-pet-technology-meant-pets-owners.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.