Dogs Go Pods: Context-dependent Access Control Rules for Sharing Personal Data of Humans and Pets

David Elia Egon Seger
University of St. Gallen
St. Gallen, Switzerland
david.seger@student.unisg.ch

Kimberly Garcia
University of St. Gallen
St. Gallen, Switzerland
kimberly.garcia@unisg.ch

Jannis Strecker-Bischoff
University of St. Gallen
St. Gallen, Switzerland
jannis.strecker-bischoff@unisg.ch

Simon Mayer
University of St. Gallen
St.Gallen, Switzerland
simon.mayer@unisg.ch

Abstract

To advance self-determined data sharing, we present a novel paradigm for *context-dependent access control for Solid*, a specification for decentralized data stores (Pods) for secure sharing of personal data. Our approach enables dynamic, real-time updates to data access rights based on contextual information such as location, proximity, and behavior. Using Bluetooth Low Energy (BLE) beacons and a mobile application, we demonstrate our contribution in a pet ownership scenario, where a BLE-enabled dog collar manages access to a dog's data Pod. For example, the owner's contact details become publicly accessible if the pet runs away; access to vaccination records are made available to customs officials when the dog crosses a country border; and additional contact information for arranging play dates is made available to other dog owners when two dogs interact frequently. Our demonstrator highlights the potential of *context-dependent access control rules* to enhance data privacy in everyday IoT environments, taking advantage of contextual triggers that can reduce end-user complexity. We discuss applications beyond pet ownership and outline future work to refine our system's usability and performance.

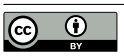
CCS Concepts

• **Human-centered computing** → **Ubiquitous and mobile computing systems and tools**; • **Security and privacy** → **Human and societal aspects of security and privacy**.

Keywords

Solid, Data Pods, Data Privacy, Decentralized Data Stores, Access Control Lists, Context-Aware, History-Aware.

ACM Reference Format:
David Elia Egon Seger, Kimberly Garcia, Jannis Strecker-Bischoff, and Simon Mayer. 2025. Dogs Go Pods: Context-dependent Access Control Rules for Sharing Personal Data of Humans and Pets. In *Companion of the the 2025 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp Companion '25), October 12–16, 2025, Espoo, Finland*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3714394.3754368



UbiComp Companion '25, October 12–16, 2025, Espoo, Finland

ACM ISBN 979-8-4007-1477-1/2025/10
https://doi.org/10.1145/3714394.3754368

1 Introduction

Internet of Things (IoT) devices that support us in accomplishing tasks are by now commonplace. We can start our vacuum cleaner even when we are not in our apartment, we can check the status of our washing machine without being in front of the device, and we can ask our voice assistant to stream our favorite TV show. Even for entities that do not produce digital data, we can now track them by, for example, attaching an Apple AirTag[1] or a Tile tracker[2] to our luggage, to our pet's collar, and even to the children in our lives [11]. This leads us to ask ourselves: *What about privacy?* What if we are wary about yet another big tech company using our data to profile us? What if we do not want to receive personalized content on how to train our dog? Or what if we do not want to get more ads telling us how terrible our dog's food is just to then receive advertisements about more expensive dog food? One of the alternatives—as proposed by Tim Berners-Lee—is to use Solid (from Social Linked Data) [14]. Solid is a World Wide Web Consortium (W3C) specification [20] for structuring data, digital identities, and accessing such data on the Web. The Solid project [16] aims to empower users to take back control of their data on the Web, so they can share it only with the applications and entities they trust. Users of Solid have a Pod (hosted by a trusted partner) in which their data is stored, and they grant and revoke access rights to process these data whenever they want.

The use of Solid is increasing, from research use cases to implementations in the real world. For example, the Flemish government in Belgium[3] is creating infrastructure to provide each citizen with a Solid Pod in which their official documents are stored (e.g., university diplomas and drivers' license); citizens can then share these official documents with specific applications, e.g., when applying for a job. In research, Solid has been used to facilitate the storing and sharing of gaze data [1], healthcare-related data [4], social media data [15], and human agent collaboration [5]. However, to transition from the current paradigm in which users' personal data is replicated, stored, and processed by each company that provides a service, to the decentralized paradigm that Solid proposes, in which users have agency on their data; it is necessary to lower Solid's usability barrier. Hence, in this work, we focus on *making it*

[1] https://www.apple.com/airtag/. Last accessed July 16, 2025.
[2] https://www.tile.com/. Last accessed July 16, 2025.
[3] https://solidlab.be/. Last accessed July 16, 2025.

easier for users to manage access and processing rights on their data, through context-dependent access control rules.

Solid uses the Web Access Control system (WAC) [17], which employs the Access Control List (ACL) model to describe, in a machine-readable and understandable way, rules for accessing and processing data stored in a Solid Pod. However, creating ACL rules requires specialized knowledge, making it unsuitable for end users. Hence, we propose a dynamic, context-dependent approach to set ACL rules. Our approach considers ubiquitous computing environments, in which users produce personal data by interacting with connected devices, leveraging cues such as location, proximity, and interaction history to design intuitive applications that seamlessly provide adequate access control according to the interactions of a user. We demonstrate our approach with a pet ownership scenario: Solid is used to store data about a dog, and the daily life of the pet serves as the basis for distributing the data to interested parties, granting and revoking rights to data based on the dog's and the owner's context.

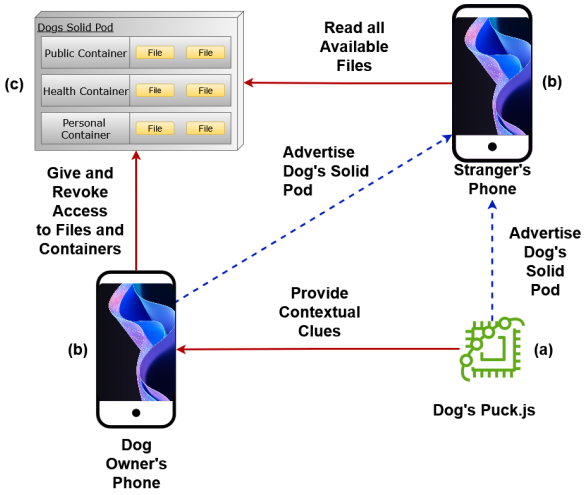


Figure 1: Overview of the prototype's components

2 Related Work

The concept of utilizing context to improve the accessibility of information is a foundational aspect of context-aware computing [2]. Jones [8] emphasizes the potential of context-aware systems in dynamically adapting to user environments, tasks, and preferences. They outline how ubiquitous computing environments enable the integration of rich contextual data, such as user activities, location, biometric sensors, and environmental attributes, to enhance information retrieval. We propose using such contextual data to support users in sharing their data.

IoT environments themselves raise substantial challenges regarding access control and privacy [3]. Qiu et al. [13] highlight three core requirements for IoT access control: policy combination, conflict resolution, and policy authoring. They show how classic methods, such as role-based or attribute-based access control, need adaptation to handle large-scale, real-time IoT data and dynamic device states. Moreover, they discuss the growing importance of context-aware attributes (e.g., user location or environmental conditions) that enable making finer-grained permission decisions. However, such elaborate permissions that ensure the appropriate data processing of which they are the subject or recipient, might increase people's *privacy labor* [22]. Thus, researchers have suggested using contextual cues to ease this burden. PriviAware [9] offers a visualization of sensor readings, paired with flexible on/off consent for data sharing, depending on context cues such as time and location of the user. A user still has to manually manage their data privacy; however, being connected to a specific context of use might make the impact of the privacy decision more tangible.

The possibilities of combining intuitive data access controls with dynamic data produced by IoT devices remain a field worth exploring further. Hence, by integrating Solid's decentralized approach with contextual data, we aim to reduce the privacy labor laid on the end user.

3 Context-Dependent Data Access Control

To showcase the potential of context-dependent data access control for Solid Pods, we propose a pet scenario, in which dogs wear a Bluetooth Low Energy (BLE) beacon on their collar, and owners use a mobile application installed on their smartphone. Smart dog collars have been used to monitor dogs' activity levels [23], to enable photo and activity sharing with their owners [25], and to connect owners with other dog owner's by recording and sharing their dogs' encounters [24]. However, researchers have pointed out privacy risks connected with such smart pet technology [6, 18] underlining the need for intuitive privacy controls. To inform pet owners about potential privacy risks, the usage of privacy labels has been suggested to highlight the data (from dogs and owners) that may be accessed or shared by a specific dog-related technology [12]. While these labels are helpful for informing pet owners about data a device might share, they are not meant to provide any data access control means. Our system proposes an implementation that allows pet owners to set rules that define which data are made available to others based on contextual factors. We consider the following situations to trigger access control rules according to the current context of the dog and its owner:

- If a dog runs away, people the dog encounters should have a way to contact its owner.
- If a dog enters a foreign country, officials should be able to read the dog's vaccination status.
- In case a dog spends a lot of time with another dog, it might indicate that the pets like each other, hence access to data for contacting the owner of the dog can be granted to, for example, set up a play date.

The project uses three central components as shown in Figure 1: (a) a commercially available BLE beacon, in our case a Puck.js [10] (see Figure 2b) equipped with several sensors, such as an accelerometer, a magnetometer, and a gyroscope, (b) an Android application, and (c) a Solid Pod hosted in our university's Solid server.

To explain the setup of our system, consider Aura, one of the authors' dog (see Figures 2a and 2b): A Solid Pod with three containers is created for Aura; each container has an ACL file, in which data access and data processing rules are described in RDF. These containers are called "public", "personal", and "health". Aside from

(a) Our test subject Aura (b) The Puck.js attached to the dog collar

Figure 2: Aura and the Puck.js attached to the dog collar.

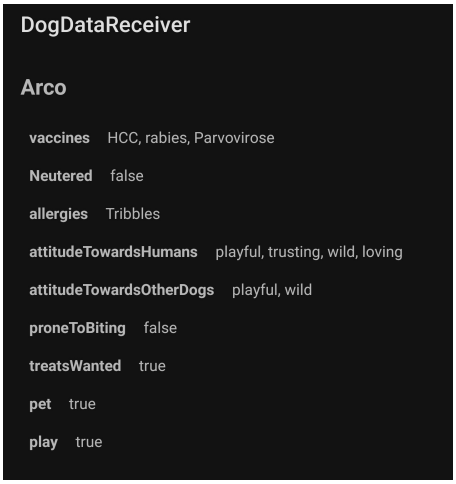


Figure 3: A Screenshot from the Android app showing the data access. When Arco is in a foreign country, the health data is readable by officials.

the ACL rules file, each container hosts JSON files with relevant information about the dog. Aura wears a Puck.js attached to her collar (see Figure 2b), which broadcasts Aura's WebID [21] (a unique identifier within the Solid server), so that the smartphone application can be connected to Aura's Puck.js. Once the device is connected to the smartphone, the advertising stops, since the Puck.js does not have the capability to maintain a connection while still advertising data. However, to ensure that the dog's data can still be discovered by strangers (e.g., dog owners of potential dog friends), even when connected to the smartphone, we switch the advertising duty to the smartphone, given that in this case, the dog is near its owner. Every 20 seconds, the Puck.js sends a ping to the smartphone, guaranteeing that the connection is still open, and that the smartphone is reachable. If this ping does not arrive for more than 40 seconds, the mobile application assumes that the dog has run away. In this case, the BLE connection in the Puck.js is interrupted, and the device resumes advertising the dog's WebID, so it can be discovered by other smartphones. The Android application continuously scans for Solid WebIDs (which might belong to unknown dogs). Once a dog is found in the vicinity, it attempts to retrieve an *Index* file from the public container. This file acts as a directory of the Solid Pod (location of files); the software traverses the directory and, one by one, attempts to retrieve files. If a file is not accessible due to access rights, the software ignores that file and continues with the next. The discovered data can then be displayed on the mobile application. Our system addresses the three situations mentioned before in the following way:

Proximity based data access If the system determines that the dog has run away from its owner, the mobile application sends an update to Aura's Solid Pod (through a SPARQL query [19]), allowing anybody that comes across her to access the "personal" container; which hosts a file with details on how to contact Aura's owner.

Location based data access To address the case in which Aura crosses a country border and foreign officials might need to check her vaccination status, the mobile application has access to the device GPS, and a Geofence[4] verifies in set intervals, if a border has been crossed. If that is the case, the mobile application sends a SPARQL update to Aura's Solid Pod, giving open access to Aura's "health" container, so it can be accessed by foreign officials.

History-aware data access. The mobile application recognizes if another WebID is discoverable for more than five minutes, and saves this interaction for future use. If this interaction happens more than five times, meaning that Aura has been spending time with a specific dog, the mobile application sends a SPARQL update to give access to this WebID to the data in Aura's "personal"container. In this way, the owner of Aura's new friend can contact Aura's owner to set a play date.

4 Validation

We attached the Puck.js to Aura's collar and went on frequent walks with her, mimicking a real-world scenario. Throughout the testing of our system, we ensured that no harm came to our canine collaborator, and that she was treated following guidelines for ethical dog-computer interaction [7]. To emulate another dog with the same setup, we used a second Puck.js and a second Android device, advertising the data of a fictional dog called Arco. In Figure 4 we see the results of meeting this second dog on a walk without any special conditions. The mobile application automatically finds Arco's WebID and reads the data that is publicly visible, which in this case corresponds to Arco's "public" container in his Solid Pod. Once we moved this fictional dog to a foreign country, people walking by are able to read his health data, as can be seen in Figure 3. Finally, we moved Arco's Puck.js out of reach of the smartphone representing the fictitious owner, which makes Arco's Puck.js broadcast his WebID. As Figure 5 shows, since Arco is in another country, his health data and the contact information of his owner are now accessible to anybody. Similarly, after Aura meets Arco multiple times, access to the contact data of Arco's owner is permanently granted to Aura.

After gathering informal feedback from a few other dog owners, they seemed to respond well to the data access rules for dogs that ran away. While there are already established technologies (such as dog microchips) for dog identification, they often require special

[4]https://developer.android.com/develop/sensors-and-location/location/geofencing. Last accessed July 16, 2025.

readers and access to governmental databases to find out how to reach a dog's owner. Having an application that can be installed on any smartphone, which automatically scans data of passing dogs, was deemed a step-up compared to the need for specialized scanners. The context-aware data access features were described as "nice to have", particularly that the contact information of a dog owner was not accessible by everybody, unless behavioral context suggests the need to give access to personal data. Some owners mentioned that access to the dog health data could also be of help, since right now people have to carry physical "dog passports" when traveling; with our proposed approach, the passport could be digitalized and only accessible in foreign countries. As for the access based on history of interactions, the owners would like to have a mechanism that allows them to have more control over the access rights, as they do not want to always share contact information just because their dog likes to play with another dog.

5 Discussion and Future Work

Our application utilizes the Solid protocol, emphasizing the decentralized and self-determined approach that aligns with Solid's mission of providing users agency on their data. While the current paradigm when using digital services relies on replicating our personal data and giving it away to big corporations, our solution enables users with no technical knowledge, to dynamically and automatically grant and revoke access and processing rights to their data considering their context. Hence, our approach could advance Solid's adoption by making it more accessible to end users.

Although our approach was demonstrated in a pet scenario, context-dependent data access could have a wider impact in industrial and other professional settings, especially, in those in which personal data are involved, such as:

- Medical data of elderly people or people at risk could be stored in their Solid Pods, and shared with first responders to access medical records based on proximity, location and any other combination of sensor data that contributes to medical care. Moreover, medical data could be shared with loved ones or close-by hospitals, in case a person at risk or an elderly person leaves their "home" zone.
- In transportation use cases, access to dash-cam videos of license plates and footage of pedestrians, can be given to the authorities when a crash occurs. In the case of self-driving cars and assisted driving, safety could be improved by sharing a car's planned behavior with nearby cars.
- At home, smart devices could adapt their behavior according to users' presence and usage. In the case of smart fridges, they could lock foods in airtight compartments, when somebody with an allergy is nearby. Moreover, continuing with the theme of pets, automatic feeders could change the amount or type of food provided, according to a specific pet and their physical activity on that day.
- In case of a natural disaster (e.g., fire, earthquake, and flooding), location data of victims, first responders, and helpful resources provided by civilians could be shared with neighbors and other organizations.
- In an industrial setting, access to production machines or specialized data could be contingent on the proximity of an experienced or novice user and the number of training hours they have achieved.

Our current prototype serves as a foundation to explore context-dependent access control. However, several limitations and possible extensions have been identified. In our current implementation, the BLE beacon does not scan for other WebIDs on its own. This is not a problem in the context of dogs, as they generally do not roam freely. To extend the application to other pets, especially cats that often move independently of their owners, WebID scanning should be implemented on the Puck.js itself. The Puck.js could scan and save all WebIDs it discovers for later retrieval by the mobile application, allowing cat owners to learn more about who their cat met during the day. The availability of the context-dependent data access could also be increased through appropriate investments in a supporting network of real-life Solid server infrastructure. For instance, dog parks could have their own Solid Pods, keeping track of which dogs are currently playing there, and if their behavior could lead to problems for other visitors. Through our approach, the system would only share data with people that actually visit the parks. Moreover, access to a pet's medical history could be given to veterinarians only if a pet is actually at the their office.

As the project mainly served as an illustration of how to implement context-driven data access using Solid, topics such as user experience and usability, battery life and performance of our prototype were not the primary focus and could be improved in a future iteration. Moreover, we plan to conduct an evaluation with more dogs and their owners to gain deeper insights into the world of smart pet ownership and pinpoint the need and usefulness of our system for real users.

6 Conclusion

Through the usage of the Solid specification, a commercially available BLE beacon, and the implementation of an Android application, we demonstrated the implementation of context-dependent data access control. We used a pet ownership scenario to showcase our approach in a real-life scenario. In our demonstrator, if conditions on location, proximity, or interaction history are met, a person coming across a dog wearing a BLE-enabled collar can access the dog's Solid Pod. To validate our implementation, we conducted a small, informal user feedback session, collecting opinions from dog owners about our system, and we presented possible fields in which this technology could be useful in the future. We reflected on the project and present various areas for improvement and possible extensions. We will continue exploring context-dependent data access, and we hope that this work serves as inspiration for furthering the cause of private data ownership using Solid Pods and beyond.

References

[1] Kenan Bektaş, Jannis Strecker, Simon Mayer, and Kimberly Garcia. 2024. Gaze-Enabled Activity Recognition for Augmented Reality Feedback. *Computers & Graphics* 119 (April 2024), 103909. https://doi.org/10.1016/j.cag.2024.103909

[2] Anind K. Dey. 2001. Understanding and Using Context. *Personal and Ubiquitous Computing* 5, 1 (Feb. 2001), 4–7. https://doi.org/10.1007/s007790170019

[3] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Yokohama Japan, 1–16. https://doi.org/10.1145/3411764.3445148

[4] Hemant Ghayvat, Munish Sharma, Prosanta Gope, and Pradip K. Sharma. 2022. SHARIF: Solid Pod-Based Secured Healthcare Information Storage and Exchange

Solution in Internet of Things. *IEEE Transactions on Industrial Informatics* 18, 8 (2022), 5609–5618. https://doi.org/10.1109/TII.2021.3136884
[5] Jan Grau, Simon Mayer, Jannis Strecker, Kimberly Garcia, and Kenan Bektas. 2024. Gaze-based Opportunistic Privacy-preserving Human-Agent Collaboration. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '24)*. Association for Computing Machinery, New York, NY, USA, Article 176, 6 pages. https://doi.org/10.1145/3613905.3651066
[6] Scott Harper, Maryam Mehrnezhad, and Matthew Leach. 2023. Security and Privacy Concerns of Pet Tech Users. In *Proceedings of the 12th International Conference on the Internet of Things* (Delft, Netherlands) *(IoT '22)*. Association for Computing Machinery, New York, NY, USA, 155–162. https://doi.org/10.1145/3567445.3571102
[7] Ilyena Hirskyj-Douglas and JC Read. 2016. The ethics of how to work with dogs in animal computer interaction. In *Proceedings of the Animal Computer Interaction Symposium. Measuring Behaviour.* 6.
[8] G.J.F. Jones. 2005. Challenges and opportunities of context-aware information access. In *International Workshop on Ubiquitous Data Management.* 53–60. https://doi.org/10.1109/UDM.2005.5
[9] Hyunsoo Lee, Yugyeong Jung, Hei Yiu Law, Seolyeong Bae, and Uichin Lee. 2024. PriviAware: Exploring Data Visualization and Dynamic Privacy Control Support for Data Collection in Mobile Sensing Research. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 787, 17 pages. https://doi.org/10.1145/3613904.3642815
[10] Pur3 Ltd. [n. d.]. https://www.espruino.com/Puck.js
[11] Jane Mavoa, Simon Coghlan, and Bjørn Nansen. 2023. "It's About Safety Not Snooping": Parental Attitudes to Child Tracking Technologies and Geolocation Data. *Surveillance & Society* 21, 1 (March 2023), 45–60. https://doi.org/10.24908/ss.v21i1.15719
[12] James McParlan and Dirk Van Der Linden. 2021. Privacy Labels Should Go to the Dogs. In *Eight International Conference on Animal-Computer Interaction.* ACM, Bloomington IN USA, 1–10. https://doi.org/10.1145/3493842.3493888
[13] Jing Qiu, Zhihong Tian, Chunlai Du, Qi Zuo, Shen Su, and Binxing Fang. 2020. A Survey on Access Control in the Age of Internet of Things. *IEEE Internet of Things Journal* 7, 6 (2020), 4682–4696. https://doi.org/10.1109/JIOT.2020.2969326
[14] Andrei Vlad Sambra, Essam Mansour, Sandro Hawke, Maged Zereba, Nicola Greco, Abdurrahman Ghanem, Dmitri Zagidulin, Ashraf Aboulnaga, and Tim Berners-Lee. 2016. Solid: A Platform for Decentralized Social Applications Based on Linked Data. *MIT CSAIL & Qatar Computing Research Institute, Technical Report* (2016).
[15] Valentin Siegert, Dirk Leichsenring, and Martin Gaedke. 2024. Trusting Decentralized Web Data in a Solid-Based Social Network. In *Web Engineering*, Kostas Stefanidis, Kari Systä, Maristella Matera, Sebastian Heil, Haridimos Kondylakis, and Elisa Quintarelli (Eds.). Springer Nature Switzerland, Cham, 230–245. https://doi.org/10.1007/978-3-031-62362-2_16
[16] Solid Project. 2025. Solid: Your Data, Your Choice. https://solidproject.org/.
[17] Sarven Capadisli Tim Berners-Lee, Henry Story. 2024. https://solidproject.org/TR/wac
[18] Dirk van der Linden, Emma Williams, Irit Hadar, and Anna Zamansky. 2020. Some might freak out: What if your dog's activity tracker were to have a data breach?. In *Proceedings of the Sixth International Conference on Animal-Computer Interaction* (Haifa, Israel) *(ACI '19)*. Association for Computing Machinery, New York, NY, USA, Article 4, 12 pages. https://doi.org/10.1145/3371049.3371057
[19] W3C. 2013. SPARQL 1.1 Query Language. https://www.w3.org/TR/sparql11-query/.
[20] W3C. 2018. Solid Community Group. https://www.w3.org/community/solid/.
[21] W3C. 2024. WebID - W3C Wiki. https://www.w3.org/wiki/WebID.
[22] W3C. 2025. Privacy Principles - Privacy Labor. https://www.w3.org/TR/privacy-principles/#privacy-labor.
[23] Gary M. Weiss, Ashwin Nathan, J.B. Kropp, and Jeffrey W. Lockhart. 2013. WagTag: a dog collar accessory for monitoring canine activity levels. In *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication* (Zurich, Switzerland) *(UbiComp '13 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 405–414. https://doi.org/10.1145/2494091.2495972
[24] Yu-chi Wu, Zhang Zhe-Wei, Wei-Ling Chung, Chien Yu-Ting, and Yuxin Chen. 2024. DOGO Smart Social Network For Pet. In *Proceedings of the Eighteenth International Conference on Tangible, Embedded, and Embodied Interaction* (Cork, Ireland) *(TEI '24)*. Association for Computing Machinery, New York, NY, USA, Article 107, 4 pages. https://doi.org/10.1145/3623509.3635862
[25] Cheng Xue, Zonglin Zuo, Xinran Jiang, and Xinyi Fu. 2024. DogChat: A Pet-centered Smart Collar Prototype based on Large Language Models and Wechat. In *Companion of the 2024 on ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Melbourne VIC, Australia) *(UbiComp '24)*. Association for Computing Machinery, New York, NY, USA, 162–166. https://doi.org/10.1145/3675094.3677606

A Screenshots

Figure 4: Screenshot of the Android app. When Arco is in his home country, only public data is accessible.

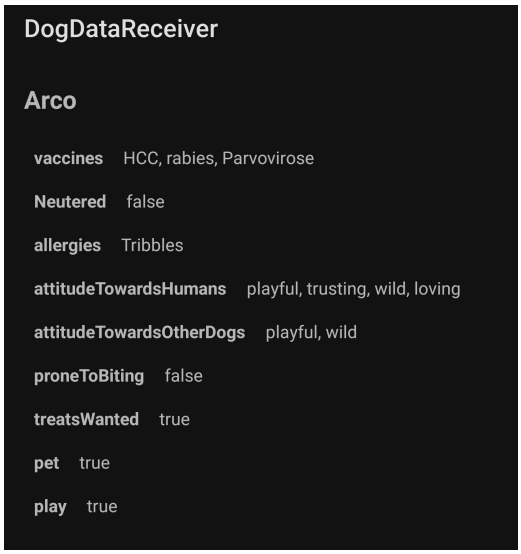


Figure 5: Screenshot of the Android app. When Arco is in a foreign country after he ran away, contact and health data is readable.