Digital Health: Changing the Way Healthcare is Conceptualised and Delivered
E. Cummings et al. (Eds.)

doi:10.3233/SHTI190765

Privacy in Aged Care Monitoring Devices (ACMD): The Developers' Perspective

Sami ALKHATIB[a], Jenny WAYCOTT[a] and George BUCHANAN[a]
[a]*Computing and Information Systems, The University of Melbourne*

Abstract. "Aging in place" refers to older adults remaining in their home as they age to maintain their independence and attachment with their community. The preference to "age in place" has led to increasing use of aged care monitoring devices to monitor the health, safety and wellbeing of older adults while living alone in their home. However, these devices raise privacy concerns as they are designed to collect, use and share sensitive data from the older adults' private life in order to provide its real-time monitoring capabilities. This study involved interviewing developers from companies that design or deploy aged care monitoring devices about how they view privacy. The study found that developers mostly link privacy to unauthorized/uncontrolled access to users' data, data security risks and human errors. We advocate aged care monitoring devices companies to expand their view of privacy and to adopt a sociotechnical approach when addressing privacy in their developed devices. This involves considering human issues when addressing privacy, rather than focusing exclusively on technical solutions for privacy problems.

Keywords. IoT, aged care, privacy, monitoring

Introduction

"Aging in place" enables older adults to maintain their independence and autonomy by remaining in their homes and communities for as long as possible rather than living in assisted living facilities [1]. However, some older adults move to residential care facilities due to the inadequacies of their homes and surroundings to meet their needs such as accessibility barriers or unavailability of necessary services and care [2]. Moving to residential care facilities is less favored by policy makers and health providers in addition to the older adults themselves, who may fear losing their independence [3]. The preference to "age in place" has led to increasing use and acceptance of aged care monitoring devices (ACMD) to monitor the health and wellbeing of older adults living alone in their home. Such monitoring devices often make use of Internet of Things (IoT) by equipping physical objects with computing resources and sensors to sense and collect data from older adults and their surrounding environment and to autonomously communicate this data via the Internet.

ACMDs raise privacy concerns similar to any Internet enabled devices. Privacy risks related to the usage of ACMD are exacerbated due to the sensitivity of the collected data and the ability of these devices to create massive personal health and behavioural records [4]. These devices are designed to collect data from the older adults and from their own homes and surrounding environments, providing a window into the user's private life [5]. Privacy has always been linked to an individual's dignity [6]. Any potential privacy infringements caused by ACMDs such as exposing sensitive details of older adult's

health or personal activities to unintended people might enhance the risks of dignitary harms for them and thus negatively impact their willingness of using these devices [7]. Therefore, it is important to understand how to protect and address privacy issues in ACMD.

1. Study Aims

Technology developers working for ACMDs companies are responsible for the design and development of these devices and incorporating privacy protections in them. However, there is limited understanding of how developers working for ACMD companies perceive privacy and interpret it. This study aims to fill this knowledge gap by conducting in-depth interviews with developers, to gain insights into how developers understand privacy and what privacy problems they believe need to be addressed in the development of ACMD. The findings of this study extend the findings of our previous literature review [8].

2. Method

This research involved in-depth semi-structured interviews with ten developers from eight companies. Participants were recruited based on the purposeful sampling approach that involves identifying and selecting individuals who are experienced and/or knowledgeable about a phenomenon of interest [9]. We used three methods to recruit participants: 1) directly approached developers in ACMD companies found from an internet search, 2) used the snowball method, where we asked participants who we interviewed to introduce us to other potential interviewees from their industry contacts, and 3) networking with people from the aged care industry by attending related conferences and asking them to refer us to developers.

Of our ten participants, four were CEOs. The other six participants worked in different positions with varying levels of experience in developing hardware and/or software for ACMD or applying business policies and practices that govern the development and usage of ACMD. Marshall et al. [10] highlighted that ten participants should be enough to provide data saturation for an in-depth qualitative study in Information Systems research.

The interviews were semi-structured – the questions provided a guide, but sometimes additional questions were asked based on participants' responses, allowing a conversation to develop organically. The questions were open-ended, providing opportunities for participants to provide as much, or as little, detail as they wanted to about the topic. Participants were asked how they define privacy and what privacy problem(s) they were aware of that require solutions in ACMD.

Interviews were conducted between June and November 2018. All interviews were audio recorded and later transcribed to create a written record of the conversations.

The interpretive approach was implemented to make sense of the interview transcripts. This involves gaining insights about a phenomenon by interpreting the meanings people assign to it [11]. Through this analysis we aimed to understand what privacy means to participants and how their views are reflected in practice. The interview transcripts will be our guide to create new insights required to answer questions on how participants perceive privacy and address it in ACMD [12].

3. Findings

In this section, we firstly discuss the various notions of privacy that interviewees had. We then discuss the key threats to privacy in ACMD they identified: 1) data accessibility, 2) security issues and 3) human errors.

3.1. Various Notions of Privacy

Although participants were informed that this research aims to explore their thoughts on privacy in ACMD, we commonly observed that they struggled to articulate a definition for privacy when they were asked to define it. Almost all participants required some time to think about an answer and seemed to be confused, not expecting such a question or not sure about what privacy means to them. For instance, "*[Exhale]…. what does privacy mean to me? aaa.. Can you…. privacy to me personally, privacy in terms of the project [trials on new devices]... my clients?"(P8); "[hem]…. I think it's [privacy] the treating of data confidential … the confidential treating of data .. treating of data…mmm .. well, in particular people are afraid of …" (P1).*

However, all participants except one responded to our question on how they define privacy by narrowing it into one or more of what they believe poses privacy problem(s) and by using these problems to conceptualise privacy. Five participants considered unauthorised access to user's data as the main problem that causes privacy breaches, while other participants linked privacy breaches to other problems such as data insecurity, lack of confidentiality, secrecy and secondary usage of data. Following are some examples of how participants used these problems to define privacy in ACMD. *"[privacy] is to protect data from being accessed by unauthorised people or third parties." (P4); "privacy means to keep things as a secret and not to allow unauthorised people access to data." (P9); "[privacy] not to be intrusive and to apply strong security measurements on data transferred to make sure no unintended people have access to it." (P3); "[privacy] is confidentiality of data and not to use it for commercial purpose." (P1).*

Two participants described privacy as having control over what to disclose or not and to whom to disclose details of their own lives. As an example, "*[privacy] is to have control over what to disclose to each person each disclosure event. To make it as simple as possible, as long as I am in control of my own thoughts, I want that control to be my own and I want to make those decisions of what is public and what is private and to have that option at each time." (P8).*

The same participant (P8) reflected this conceptualisation of privacy in ACMD as gaining consent from older adults to start collecting their data after clearly explaining what will happen to it: *"People who agree to be part of this project [trials on their developed aged care monitoring device] need to consent and agree that there will be people within the organisation that will be reviewing their data specifically for the purpose of the project." (P8).*

However, one participant insisted that privacy has no definition. According to this participant, privacy is something that individuals trade-off in return for what they get from services: "*It is difficult to define privacy these days! It's more about what will you get in return for losing your privacy." (P10).*

3.2. Threats on Privacy

Participants were asked to identify privacy problems in ACMD, to explore what privacy problems developers believe need to be addressed in their devices. Participants identified three types of threats they believed were the main reason for privacy problems in ACMD: 1) uncontrolled data accessibility 2) security risks and 3) human errors.

3.2.1. Data Accessibility

Five participants mentioned uncontrolled data accessibility as the main threat on privacy in ACMD. Participants indicated that access to users' data should only be granted to legitimate stakeholders to accomplish a predetermined purpose [13]. The following are examples: "*the weakest point is who has access to data and can export files and so."(P2); "the other risk is the care portal access and who has access to their care portal, how are we tracking who accesses the portal and whether there are malicious intents." (P9); "if more people have access to this data how are we going to control access to this data to make sure that the data is kept safe." (P4).*

3.2.2. Security Issues

Three participants pointed out data insecurity as the main threat on privacy in the use of ACMD. They noted that transferred and stored data are exposed to security threats: "*transferring data is the weakest point in terms of privacy as it can be hacked." (P3); "network transmission area, it's outside your realm and control. Denial-of-Service and these things have to be considered." (P7); "The weakest point in ACMD in terms of privacy is where the data is stored and protected." (P1).*

Hacking is to gain access to users' data in order to commit malicious activity [14] and denial-of-service (DoS) is an attack in which the attacker shuts down a computing machine or network by making it inaccessible to its intended users [15]. Transferred and stored data can be protected from malicious attacks by incorporating robust security protection models [16].

One participant suggested that using strong passwords and enforcing the change of default passwords for users on ACMD is a useful technique to protect users' data on different levels starting with the collected data, transferred data and wherever it gets stored. This participant's suggestion could be considered as protecting against uncontrolled accessibility to user's data, but we have categorised it as a data security solution as it was mentioned in the context of protecting users' data from malicious attacks. Data accessibility is more related to the mechanisms, policies and laws applied in order to regulate stakeholders' access to users' data. This can be seen in the following comment "*we do not use as an example default passwords, everyone gets a random generated password with validity on it. So I believe the weakest point is the credentials used to access data no matter on which side." (P4).*

Nevertheless, one participant (P5) highlighted that even if data successfully gets compromised, as long as the same data is de-identified and/or does not contain personal details, the compromised data will be meaningless and will not cause any harm to its owners: "*sensors do not provide any meaningful data, the same thing applies on data stored on the hub, no data is identified, no names no personal data."*

De-identifying users' data is important as an extra protection layer in case data gets revealed. However, overreliance on de-identification to protect users' health data is risky

as it depends on whether enough information is removed from users' records to make their data harder to re-identify [17].

3.2.3. Human Error

Two participants mentioned employees' errors and behaviors when dealing with stored and processed data as a major threat to users' privacy. Participants specifically highlighted employees who have access to users' data and are permitted to modify or transfer it. Human errors can be unintentional such as sending reports containing sensitive data via email to unintended recipients by mistake, or intentional such as sharing passwords between employees to access users' data required for certain tasks [18]. The following are examples from participants' responses related to human errors: "*Human error is the main threat to privacy especially who has access to data stored on cloud." (P5); "Human errors and week passwords are the main threats on privacy."(P2).*

4. Discussion

We found that developers working for ACMD companies perceive uncontrolled/unauthorized access to users' data as the major threat on older adults' privacy with security concerns coming after it. The main difference between the findings of this study and our literature review [8] is introducing "human errors" as a serious problem to users' privacy in ACMD. Privacy breaches in organisations that are attributed to human errors are increasing [19]. Examples of human errors are accidental disclosures of users' data, improper behaviors by employees or mistakes due to following an inadequate plan or procedure [20].

Additionally, we observed that participants struggled or showed discomfort when asked to define privacy [21]. This might indicate that developers working in ACMD companies are not well prepared, have little information on privacy or treat it as a marginal topic. We contend that ACMD companies should adopt an expanded view of privacy. Claiming that older adults' privacy is protected by providing solutions to secure users' data or human errors means that there will remain other privacy loopholes. Solove [22] likened privacy to a recipe. Using only some ingredients and leaving out other ingredients means that privacy will be partially baked. Therefore, it is important to find the right recipe to ensure ACMD companies do not leave out key ingredients. The General Data Protection Regulation (GDPR) applied in the EU provides clear guidelines that can be used by ACMD companies to provide a better understanding of privacy aspects and to avoid neglecting any privacy problem(s).

5. Conclusion

Most of the participants described privacy as a concern and showed interest in finding effective solutions to privacy issues in ACMD. However, we found that ACMD companies need to improve their developers' awareness and understanding of privacy and to adopt a comprehensive view of privacy issues in ACMD. Therefore, we advocate ACMD companies to tackle privacy in a sociotechnical [23] approach by considering the human factors in addition to providing technical solutions to privacy problems such as data insecurity and identification. This requires ACMD companies to ensure that their

employees get effective training and comply with strict privacy policies [19]. As such, companies are required to collect older adults' privacy requirements and to conduct tests on their developed ACMD to determine whether their developed devices address older adults' privacy concerns.

References

[1] Wiles, J. L., Leibing, A., Guberman, N., Reeve, J., & Allen, R. E. (2012). The meaning of "aging in place" to older people. The gerontologist, 52(3), 357-366.
[2] Iecovich, E. (2014). Aging in place: From theory to practice. Anthropological notebooks, 20(1), 21-33.
[3] World Health Organization (WHO). (2018). Aging and Life Course. Retrieved from https://www.who.int/ageing/en/
[4] Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS quarterly, 35(4), 989- 1016.
[5] Mittelstadt, B. (2017). Ethics of the health-related internet of things: a narrative review. Ethics and Information Technology, 19(3), 157-175.
[6] Sharkey, A. (2014). Robots and human dignity: a consideration of the effects of robot care on the dignity of older people. Ethics and Information Technology, 16(1), 63-75.
[7] Gururajan, R., Toleman, M., & Soar, J. (2004). Necessity for a new technology acceptance model to predict adoption of wireless technology in healthcare. HIC 2004: Proceedings, 87.
[8] Alkhatib, S., Waycott, J., Buchanan, G., & Bosua, R. (2018, August). Privacy and the Internet of Things (IoT) Monitoring Solutions for Older Adults: A. In Connecting the System to Enhance the Practitioner and Consumer Experience in Healthcare: Selected Papers from the 26th Australian National Health Informatics Conference (HIC 2018) (Vol. 252, p. 8). IOS Press.
[9] Cresswell, J. W., & Plano Clark, V. L. (2011). Designing and conducting mixed method research. 2nd Sage. Thousand Oaks, CA.
[10] Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research? A review of qualitative interviews in IS research. Journal of Computer Information Systems, 54(1), 11-22.
[11] Spiggle, S. (1994). Analysis and interpretation of qualitative data in consumer research. Journal of consumer research, 21(3), 491-503.
[12] St George, S. (2010). Applied interpretation: a review of interpretive description by Sally Thorne. The Qualitative Report, 15(6), 1624-1628.
[13] M. Henze, R. Hummen & K. Wehrle, The cloud needs cross-layer data handling annotations. In Security and Privacy Workshops (SPW), 2013 IEEE, (2013), 18-22.
[14] Schclar, A., Rokach, L., Abramson, A., & Elovici, Y. (2012). User authentication based on representative users. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 42(6), 1669-1678.
[15] Chen, H., Liu, M., & Zhongchuan, F. (2019). Using Improved Hilbert–Huang Transformation Method to Detect Routing-Layer Reduce of Quality Attack in Wireless Sensor Network. Wireless Personal Communications, 104(2), 595-615.
[16] Su, C. J., & Chiang, C. Y. (2013). IAServ: An intelligent home care web services platform in a cloud for aging-in-place. International journal of environmental research and public health, 10(11), 6106-6130.
[17] Culnane, C., Rubinstein, B. I., & Teague, V. (2017). Health data in an open world. arXiv preprint arXiv:1712.05627.
[18] Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. Applied ergonomics, 38(2), 143-154.
[19] Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. Journal of Information Privacy and Security, 8(2), 33-56.
[20] Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. computers & security, 28(3-4), 215-228.
[21] Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S., & Balissa, A. (2018). Privacy by designers: software developers' privacy mindset. Empirical Software Engineering, 23(1), 259-289.
[22] Solove, D. (2018). Why I Love GDPR: 10 Reasons. Retrieved from https://teachprivacy.com/why-i-love-th e-gdpr/
[23] Notario, N., Crespo, A., Martín, Y. S., Del Alamo, J. M., Le Métayer, D., Antignac, T., ... & Wright, D. (2015, May). PRIPARE: integrating privacy best practices into a privacy engineering methodology. In 2015 IEEE Security and Privacy Workshops (pp. 151-158). IEEE.