Is It Just Steps and Calories? Elementary School Students' Conceptualization of Ownership and Privacy of Self-Tracking Data

Andria Agesilaou and Eleni A. Kyza
aa.agesilaou@edu.cut.ac.cy, Eleni.Kyza@cut.ac.cy
Cyprus University of Technology

Abstract: Children are reported to have limited knowledge of where, why and by whom their data are being (re)used. This study examined students' understanding of personal digital data, and the reasons they are willing to concede personal data ownership. Data were collected from an educational intervention with 63 elementary school students. Results indicate that students' awareness of the commercial use of their personal data is not well-developed and that ownership of data varies according to context.

Introduction

Children are reported to have limited knowledge and understanding of where, why and by whom their data are being collected or how their data are being treated and (re)used (Pangrazio & Selwyn, 2019). We argue that psychological ownership towards personal digital data is a key construct in empowering students to understand their contributions to the Big Data era. Even though children understand ownership from a young age, employ protective strategies towards owned physical objects, or show resistance or denial to share or lend objects (Nancekivell et al., 2013), there is scarce research showing if and how they can employ the same protective strategies for their digital traces. This study examined children's understanding of data ownership through their engagement with scenarios embedded in an inquiry curriculum to help them reason about their own personal digital data. The following questions were investigated: (RQ1**)** What are upper elementary school students' affective, behavioral and cognitive states towards personal digital data privacy? (RQ2**)** How do students conceptualize ownership of their own digital data? and (RQ3**)** Under which circumstances are students willing to concede personal data ownership to third parties and how do they explain these decisions?

Methodology

This study employed a qualitative methodology. Participants were 63 students (32 girls) from one fifth and two sixth grade classes from the same school. Each student was provided with an activity tracker adjusted to his/her personal information (gender, year of birth, height and weight) offering the opportunity to collect and critically consider data from their own physical activity. The curriculum progressed from familiarizing students with activity trackers through experiential activities (lesson 1), to the exploration of three hypothetical scenarios, presented by the director of a company that develops and sells activity trackers and explored through a gamified approach (lessons 2-3). These scenarios are: (A) A sports company requests access to students' personal tracking data to send them discount coupons based on their activities; (B) A health insurance company asks for a student's heart rate data to decide whether to cover medical expenses to treat her heart disease, and (C) A children's gym gave their members a free activity tracker and is now asking for their permission to post their data on a members' only website, in exchange for their inclusion in a monthly competition for free subscriptions to the gym. Students in each class worked in four groups of six students each (12 groups in total). Data were collected via pre- (n=22) and post-intervention interviews (n=15) and videos of two student group in-class discussions. Two coding schemes were employed to the interviews to identify students': (1) Affective, Behavioral, and Cognitive states towards personal data privacy practices (Chi et al., 2018) and (2) conceptualization of ownership.

Findings

RQ1: What are students' affective, behavioral and cognitive states towards their personal digital data?

***Affective states*:** Students choose to disclose their personal data on their social network accounts for *communication* and *socializing* purposes, something that is reported to make students happy (n=7). Negative affective states were related to possible personal data violations through hacking of social networking accounts. Students reported they would feel anger, fear, stress and be offended if faced with such situations.

Behavioral states: Students protect their personal data online to avoid *data violations from hackers, hazardous communication with strangers,* and *disclosure of location information.* Students reported one (n=6) or

more (n=7) of the following behaviors: having strong passwords, having private accounts and sharing only with friends and people they know, using a pseudonym, and avoiding uploading photos that show someone's face and reveal its identity. When asked how they decide what to disclose and with whom, the vast majority (n=18) reported they do not share anything with strangers and avoid sharing information that reveals their location (n=14).

Cognitive States: Students believe that their data are used for negative purposes (n=8), by hackers (n=7), for bullying purposes using their photos (n=8), by the police (n=2), etc. Only three students in the pre-intervention interviews reported that their data can be used by the companies who develop the applications students use. This number increased to eight after the learning intervention, highlighting the potential of such educational efforts to positively affect students' awareness of personal data mining.

RQ2: How do students conceptualize personal data ownership?

Table 1 presents how students participating in the post-intervention interviews conceptualized ownership of self-tracking data in relation to the three hypothetical scenarios. Students were not aware that by allowing a commercial entity to access personal data one also concedes data ownership and the rights to their personal data. These results suggest that future efforts should focus on helping students acquire a better understanding of the process of ownership transfer to third parties and the analysis and profiling of their personal data, and develop the capacity to decide which privacy protection practices they wish to employ.

Table 1: Students' conceptualization of data ownership after the learning intervention

Categories	Scenario A	Scenario B	Scenario C
Students as the only data owners	12	10	9
Shared ownership with the activity trackers company	2	1	0
Shared ownership with 3rd party (sports/insurance company, gym owner)	0	3	4
Other	1	1	2

RQ3: Are students willing to concede personal data ownership to third parties?

Students' willingness to concede ownership of personal data was dependent on *the nature of the personal data being shared*, *how they would be used*, *by whom* and *for what purposes*. These aspects shaped the group decisions to the scenarios. Students were positive in conceding data ownership to the sports company (9/12 groups) and the insurance company (12/12 groups), but negative to conceding data ownership to the gym (9/12 groups). Students also reported that they perceive self-tracking data as less important than their online conversations.

Discussion and conclusions

This study contributes to our knowledge of how elementary school students conceive the role of personal data in the context of everyday life; it can also inform the design of educational materials aiming to develop students' competencies for understanding the impact of their digital traces. Results indicate that even though students are aware of what personal data are and employ some privacy-protection tactics, they demonstrate weaknesses in understanding the data flows and in making sense of why or how their personal data might be valuable to others. At the end of the intervention, students developed a sense of ownership towards their personal data related to the "first-owner" view of property (the first person seen to possess an object is the owner, Friedman, 2008), since they are the first generators of those data. Students evaluated the flow of personal information based on certain criteria and this impacted their willingness to protect or disclose personal information, and thus concede data ownership to third parties. However, students' inability to make connections with how businesses exploit their personal data, undermines their privacy rights and reflects the need to enhance their personal data privacy skills.

References

Chi, Y., Jeng, W., Acker, A., & Bowler, L. (2018, March). Affective, behavioral, and cognitive aspects of teen perspectives on personal data in social media: A model of youth data literacy. In *International Conference on Information* (pp. 442-452). Springer.

Friedman, O. (2008). First possession: An assumption guiding inferences about who owns what. *Psychonomic Bulletin & Review*, *15*(2), 290-295.

Nancekivell, S. E., Van de Vondervoort, J. W., & Friedman, O. (2013). Young children's understanding of ownership. *Child Development Perspectives*, *7*(4), 243-247.

Pangrazio, L., & Selwyn, N. (2019). 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media and Society*, 21(2), 419–437.