INTERNATIONAL DESIGN CONFERENCE - DESIGN 2018
https://doi.org/10.21278/idc.2018.0461

NOVICE DESIGNER'S LACK OF AWARENESS TO CYBERSECURITY AND DATA VULNERABILITY IN NEW CONCEPT DEVELOPMENT OF MOBILE SENSING DEVICES

E. Kim, M. B. Jensen, D. Poreh and A. M. Agogino

Abstract

As more mobile sensing devices are introduced in the market, the risks associated with cybersecurity increase. Our research goal is to shed light on novice designers' awareness to these risks with a focus on the sensing device design. We coded qualitative data from design thinking student teams at the University of California, Berkeley to see how carefully they took data vulnerability of their created solutions into account. The results reveal that novice design students did not pay much attention to the data vulnerability of their new solutions, in spite of numerous prompts for them to do so.

Keywords: human centred design, design practice, design education, cybersecurity, data vulnerability

1. Introduction

As consumer mobile sensing (Choudhury et al., 2008) and robotic technologies mature (e.g., Jibo, 2017; Amazon Echo and Alexa, 2017; iPatrol, 2017; Google Home Mini: Seifert, 2017; Sony Aibo, 2017), it is anticipated that robots will operate in the vicinity of humans, thus directly interacting with them on a wide range of tasks in domestic settings including cleaning, climate control, monitoring, education, entertainment, healthcare (Kemp et al., 2007). Co-robots (collaborative robots that are designed to collaborate with people) will become part of our daily life in the near future and they will play important roles in human society. For example, in the field of autonomous vehicles, manufactures in Silicon Valley are studying how co-robot cars will be communicating with drivers, passengers, pedestrians, and other cars by utilizing rather simple yet useful prototypes (Said and Baker, 2017). Mobile sensing and co-robots are emerging technologies that are predicted to have exponential growth in the market (Kumar, 2017; Tao, 2017). To accomplish their tasks, such co-robots, as well as personal digital devices, may need to collect sensitive information about users or their environments. In this context, it would be problematic if co-robots are hacked or otherwise compromised.

Security and privacy risks can be significantly high when it comes to vulnerable populations such as those with lower educational levels or lower socioeconomic status users (Redmiles et al., 2017) and children where the effectiveness of existing cybersecurity awareness campaigns to foster secure user behaviours is questionable (Bada et al., 2014; Lomas, 2018). Many examples of careless user behaviour can be found regarding security practices in private and public institutions such as utility providers, public schools and even during the USA election (Denning et al., 2009; Lee et al., 2015; Jensen et al., 2016). Furthermore, children can be more vulnerable and careless, as they do not have a fully mature understanding on data security yet; they do not know how vulnerable it is to share their private data (e.g., pictures, videos, or message logs) with others (Hurst, 2018).

In order to prevent careless user behaviour two challenges need to be addressed: (1) How to increase the awareness of cybersecurity and data creation risks with users, and (2) How to inculcate designers of future connected devices (including the current generation of product design students) to include considerations of cybersecurity in their design. In a previous pilot study, interviews and observations with college students, young professionals, and young parents *(N=12)*, we found that most commercial products purchased in the current co-robotic market are used in niche circumstances: monitoring pets, children (e.g., nanny cams), and security in public areas (surveillance cameras) to uncover suspicious activities. We found that users expect mobile monitoring devices to be user-friendly, error-proof and provide immediate alerts or notices to potential problems. They desire the ability to easily turn on and off the sensing functions. They tended to criticize the functionality of current solutions and reported unfavourable user experiences in that mobile robots seemed intrusive or lacked mobility in cluttered or rough terrain. Surprisingly, they seemed willing to trust the designers and manufacturers of connected home devices to have adequately built in appropriate security (Cerrudo and Apa, 2017).

Recent studies show that U.S. universities have been failing in cybersecurity education in both undergraduate and graduate programs (Matheny, 2016; Security Magazine, 2016). Thus, in order to evaluate how well design students include cybersecurity in their research and design of mobile sensing products, we developed a design thinking course at UC Berkeley where students faced the challenge of reimagining mobile sensing with prompts to keep cybersecurity in mind. After introducing weekly prompts (throughout the six week timespan) on cybersecurity, we evaluated the results of the student teams' customer research, intermediate concepts and final prototypes in taking private data security into account. In the following section our research methodology is described. Next Section 3 describes our analysis of the collected data (weekly and final reports, and final prototypes) from student teams. The findings lead to the recommendations outlined in Section 4 calling for further research needs on how to create awareness on cybersecurity and data creation in connected products among novice designers. Discussions are included in Section 5 to reflect on the setting of the design challenge and potential impacts of research. Finally, the paper ends with conclusions and future research.

2. Research method

The goal of this research is to shed light on the awareness of cybersecurity among novice designers as well as gain insights into the challenges associated with increasing this awareness among both designers and users in order to secure safety of private data in future connected products. This preliminary study approached this topic from an explorative perspective using a summer design course at the University of California at Berkeley as a case study with interventions throughout the course. The course description, the participants, and the interventions from the teaching staff are described below. Furthermore, the data used for the analyses covering the final products as well as milestone presentations are described.

2.1. Test-bed: Summer design course

The summer course took place at UC Berkeley in early July 2017. The student teams – 27 students in six teams – worked on a 'reimagining mobile sensing' design challenge over a six-week-long course that covered the design thinking process developed by theDesignExchange (theDesignExchange, 2017). The course was organized around five design thinking modules: Research, Analysis, Ideate, Build, and Communication. The course description is provided as below.

2.1.1. Design Thinking: Methods, Skills, and Mindsets (DesInv. 390-001)

The goal of the Design Thinking course was to learn principles and methodologies of design thinking, human-centered design, and product development in a real world context. Most design and engineering professionals work under tremendous time pressure and do not have an opportunity to reflect on the development process. In this course, the stress level is low enough to allow time to experiment and learn. Teams of four-five students have the opportunity to work with students from multiple disciplines. Students have opportunities during the first two classes to scope out their possible project direction, objectives and develop team dynamics. Students were not graded on their adherence to the project theme; rather they were graded on their understanding of the human-centered design process. They were prompted to consider various aspects of mobile security as part of their process. The teaching staff and the project sponsor advised students on this topic and helped reorient teams when their designs did not address this topic. The goal was for students to create original solutions with cybersecurity in mind, with an emphasis on the human-centered innovation process. The design challenge topics and sample questions we shared with student teams are summarized below.

2.1.2. Design challenge topic: Reimagining Mobile Sensing

The project sponsor introduced the topic "Reimagining Mobile Sensing" during the first class for fifteen minutes. During the presentation of the challenge, the sponsor showed several examples of existing technologies and commercial products in this space, such as a nanny cam, discrete surveillance cameras, and Google glasses, to name a few. The design challenge in this class was framed to allow student teams to conduct customer research to create new concepts in "mobile sensing" products/services that met the teams' target user needs by addressing the following research methods and questions:

- Apply design thinking methods learned throughout the class.
- Identify new market opportunities in the teams' targeted user space.
- Identify how sensitive personal information is generated and shared between humans and the IoT connected co-robots.

2.1.3. Sample questions provided with student teams

- What kind of sensitive information is likely to be generated by human-mobile sensing robot interaction?
- What are the new market opportunity areas that users can exploit mobile sensing in their daily life or in particular types of events?
- What are user's and stakeholder's perceptions of the risks involved with associated data?
- Under what circumstances are mobile sensing systems vulnerable to attacks?
- What are effective ways of warning users when creating sensitive information and making them aware of the potential risks of leakage of this information?

2.2. Demographic of participating students in the design challenge

Twenty-seven students from different demographic backgrounds were enrolled in the class to address the given cybersecurity design problem.

- **Gender:** 15 males and 12 females
- **Nationality:** 14 domestics, 15 internationals
- **Majors:** 12 engineering, 4 architecture, 4 cognitive science, 1 economics, 2 business, 1 mathematics, 3 letters & science
- **Undergraduate Year:** 16 upper-levels (senior or junior), 11 lower-levels (freshmen or sophomore)

2.3. Data collection

We collected weekly reports that were meant to be reflective summaries of team progress with a review of how the project had progressed as a group and impacted their design outcomes within each of the five modules. Teams justified why and how they decided to select particular methods and described the results and outcomes resulting from use of each method. They were asked to include all meaningful insights in order to comprehensively discuss what they had learned and formulate next steps within the context of the design challenge.

Table 1 gives an overview of concepts and their descriptions from six student teams.

Table 1. Overview of concepts and their descriptions: Design challenge in reimagining mobile sensing

Team #	Team Name	Concept Description
1	Tobi	An automatic trash disposal machine aimed at simplifying the lives of undergraduate students and leaving them more time to devote to their studies.
2	Medical Box	A medical box that can send data and real-time feedback to the doctors and family members of a home patient in order to help them track the patient's use of prescription drugs, as well as to keep the family connected.
3	Virtual Berkeley	A solution to connect students instantly to campus, community, and social resources through eliminating the existing psychological and structural barriers with mobile sensing and crowd-sourced data.
4	Lux Viam	An augmented reality (AR) safety network that utilizes the existing framework of street lamps to increase safety and security through smart navigation.
5	BART BFF	An app to enhance the experience of Bay Area Rapid Transit (BART) users who regularly rely on BART to commute to their destinations by providing, among other things, user-tailored information about stops and departure/arrival times.
6	Fire Away	A solution to automate and simplify the process of detecting and extinguishing fires to ensure users' safety while preventing loss of users' possessions.

3. Data analysis and results

The data were analyzed and synthesized by the course teaching staff: one course instructor and two teaching assistants. To assess cybersecurity awareness, content analysis was performed with the results from both the human-centered research and the design challenges. The results have shown that novice design students' awareness and internal incentives for paying attention to the vulnerability of the new solutions was overruled by other more compelling user needs. Thus we are concerned that future product designers will overlook the potential danger that could arise due to hacking.

3.1. Data analysis

We analyzed the data collected in the format of *weekly reports* submitted by each student team over five modules of the design process as well as the final reports and prototypes turned in at the end of the course. During the course, four prompts were given to student teams to encourage them to continue considering vulnerability throughout the design process. We gave students the challenge of designing a meaningful mobile sensing robot, while keeping cybersecurity risks in mind. We gave multiple prompts to consider cybersecurity in creating new solutions. We analyzed how much they took vulnerability of their created solutions into account. Several prompts (Table 2) were made by the teaching staff and a design challenge sponsor throughout the course. Despite several prompts made to the student design teams, the result showed that the students only focused on the positive aspects of their design solutions and opportunities for use of mobile sensing technologies with very little awareness about cybersecurity issues.

Table 2. Prompts made to the student design teams over the course

	Description
1st prompt	***Design challenge announcement*** The first prompt was made in the design challenge announcement by the invited project sponsor, who was leading a cybersecurity research project, in the first week of the course. The announcement included: 1) Introduction of the design challenge, 2) Showing examples of commercial mobile co-robots, 3) Sample questions students should address, and 4) Possible target markets/populations.

2nd prompt	***Peer-review I*** The 2nd prompt was made in the first peer-review session during week 2. Student teams were asked to revisit the design challenge description and address cybersecurity issues in the research phase.
3rd prompt	***Teaching leadership's team check-in*** Each student team was revisited by one member of the teaching staff. The teaching staff member was asked to remind the student team to include any issues that the teams had been struggling with in addressing potential risks on the collected data in their new design solutions.
4th prompt	***Peer-review II*** The 4th prompt was made in the second peer-review session during week 4. Student teams were asked to revisit the design challenge description and address cybersecurity issues in the research phase.

3.2. Results

In evaluating the reports, the intensity of the attention to data vulnerability was determined by the teaching staff (the course instructor and teaching assistants) in columns 4-9 (Table 3). Three levels of ratings (low-, med-, or high) were used to codify both the frequency and intensity of words associated with cybersecurity.

Table 3. Weekly lectures and prompt/interventions made by each week

Week	Module	Prompt/ Intervention	Team 1	Team 2	Team 3	Team 4	Team 5	Team 6
Week 1	Research	***1st prompt: Announcement*** Announce the design challenge.	Low	Low	Low	Low	Low	Low
Week 2	Analysis	***2nd prompt: Peer-review I*** Ask teams to revisit the design challenge description.	Low	Med.	Low	Low	Low	Low
Week 3	Ideate	***3rd prompt: Check-in*** Provide verbal feedback to each team via a check-in.	Low	Med.	Low	Med.	Low	Low
Week 4	Build	***4th prompt: Peer-review II*** Ask teams to revisit the design challenge description.	Med.	Low	Med.	Low	Low	Low
Week 5	Communicate	-	Med.	Low	Low	Med.	Low	Low
Week 6	Final Presentation/ report	-	Low	Low	Low	Low	Low	Low

Although the student teams demonstrated creative and innovative ideas around design opportunities associated with mobile sensing, they failed to account for possible security risks associated with their solutions. Most teams focussed on creating technological solutions to problems their potential customers expressed, but little, if any, focussed on data security around the use of these products. Our observations support findings from previous research (Bada et al., 2014) that most current cybersecurity campaigns have not led to improved cybersecurity behaviour change. Similar assumptions may apply to the designers whose primary role is to produce solutions that better serve users with advanced functions and experience, but not to develop adequately secured solutions unless security itself was the goal of the product.

One student team described their concept idea in a weekly report without any notion of data security. The goal of the project of the student design team was to control lighting at night to provide a pathway to the user's destination.

> *"We envision a mobile application where users can input a destination and will be guided by a Lux Viam, or a road of light. By networking street lamps, we can create a chase pattern of light which will allow for users to keep their attention on their surroundings, and still know where to go. This system would also be active monitoring and will be able to reroute users accordingly."*

The team reported no concerns about revealing a user's intended path for walking at night, despite the fact that the campus had been experiencing a series of armed robberies and sexual attacks. Another team commented:

> *"We presume that if the convenience (of their product offering) outweighs the perceived risk of a given, more convenient method of transportation, the student (users) will likely take that method (solution)."*

When the benefits of a new solution (with advantages in convenience, cost, or time savings) outweigh the potential risks around it, the student design teams tended to disregard the potential cybersecurity risk. For instance, a team who created a solution to simplify the process of detecting and extinguishing fires, particularly for those with disabilities, the cybersecurity of the personal data collected from mobile sensing devices was dominated by the potential to save lives or reduce injury. In this case, data security was not an issue to either the student teams or the potential beneficiaries (users) of the solution. These patterns were observed throughout all teams that participated in the design challenge. None of teams in the design challenge identified user needs or pain points associated with data security or privacy. The teams appeared to not have even asked relevant questions in their interviews.

Our experience with product design students failing to understand and adequately addressing cybersecurity risks in designing new co-robotic and mobile sensing products is consistent with recent reports of practices in industry where the priority is to bring products to market quickly without adequately addressing known cybersecurity risks, even though it is arguably more feasible and cost-effective to address such security risks earlier on in the product lifecycle (Markoff, 2017). These unsettling observations taught us a valuable lesson that led us to consider the following two aspects as future research directions.

3.2.1. Educational aspects: Ease of use vs. cybersecurity

Users, including future designers, lack adequate awareness of cybersecurity risks associated with the information being collected and distributed in mobile sensing and co-robotic devices. These aspects could be addressed through educational materials targeting end users who will be using the product and designers and engineers who will be developing the product and commercializing it to the marketplace. Use scenarios show a trade-off between usability and secure data features. Most U.S. universities have little focus on cybersecurity in their engineering curriculum (Matheny, 2016; Security Magazine, 2016). This triggers a need to develop design guidelines and educational materials to embed more cybersecurity topics into product design courses so that cybersecurity and usability are equally prioritized in a way that reduces the cost of including secure data features.

3.2.2. Comparative research across different user populations, different application areas

We found a need to investigate different levels of awareness and thresholds of the technology adaption by different demographic groups and different application areas. As technologies are advancing and providing more benefits to users over time, the application areas of co-robotics and mobile sensing will be growing and broadening, just like the variety of new solutions that student teams came up with over the six-week design challenge: a smart home trashcan, a smart medical pill box, a social app targeted to international students, AR safety lights on campus, improved transportation and a smart fire alarm for disabled users. We are investigating whether there are underlying and/or distinct types of data security risks on new product offerings across different user populations (e.g., college students, young professionals, elderly, parents with children, etc.) and different application areas (e.g., personal, social, medical, productive, etc.). One example from our preliminary research, revealed that children were more likely to perceive robots as positive companions to provide pleasurable experiences whereas college students were more cautious and critical.

> *"For the kids, they love interacting with it [co-robot]. Just one camera movement gets them really excited and they wave and say "hello" as if it's an actual person."* – a mother with 2 children

> *"I just don't see how practical this is. I mean why not just get a surveillance camera that gets a wide view of the entire space."* – a senior male college student

4. Recommendations

4.1. Human-centered research in cybersecurity

The security of sensitive data is only as strong as the weakest link, which often turns out to be the human user and not the firewall. This makes the users' awareness of the data created as well as the risk connected with data breach critical. Hence there is a need to address the challenge from a human-centric research perspective to understand and highlight users' awareness, motivations and behaviour in the context of cybersecurity (Dunn Cavelty, 2014). Changing users' behaviours in cybersecurity requires substantial efforts and relies on various factors: personal, social environmental, and cultural factors (Bada et al., 2014). Past research on users' perceptions of mobile robots has been conducted before, but did not focus on cybersecurity issues. For example, Ju and Takayama (2009) explored how users perceive an automatic door when varying modes of movement. Yang et al. (2015) presented an experiment to examine how people in public areas interact with everyday objects using the mobile trashcan prototype as a touch point between people and the object. However, these experiments focussed on investigating the overall user experience and usability around the mobile robots and not data security issues.

More research is needed to help designers identify where to focus, particularly with emerging co-robotic and mobile sensing products. Are private users aware of the sensitive data created when interacting with home-robots? Do they know how to protect themselves from cyber-attacks? Where do potential cybersecurity threats arise? What motivates cybersecurity awareness – data awareness or consequence/risk-awareness? By utilizing extensive methods and tools in human-centered design in the field of advanced technology interactions, we envision generating a deep understanding of what kind of sensitive information is vulnerable to breach and requires risk mitigation. Information can be unconsciously transferred from daily life to mobile sensing devices or co-robots, without caution. Further, a mapping of users' awareness about security-related issues needs to be addressed using a user-focussed, rather than technology-driven approach in order to achieve successful adoption of safe co-robotic systems in human daily life.

4.2. Creating cybersecurity guidelines for future designers and engineers

There is a growing demand for teaching data security content in higher education (Grose, 2018). For example, UC Berkeley has recently announced an online cybersecurity master's degree on campus to provide interdisciplinary learning contents on technical challenges, social and ethical issues, particularly around online cybersecurity (Public Affairs UC Berkeley, 2017). What we are still missing, however, are opportunities to educate future designers of physical hardware products along with the web security. Current solutions to prevent data security breaches tend to be short-sighted and do not focus on the underlying needs associated with end users. While banning the use of mobile devices from children, for instance, might be one solution for tackling the problem, it neglects the potential benefits of mobile devices for children and their parents. Hence, it is timely to apply human-centered design methodologies to better understand information security risks among consumers and educate the next generation product designers whose increased awareness and motivation around cybersecurity issues could have long-term impact. The recent news on Mr. Zukerberg's action to tape up the camera and micro jack on his MacBook (Rogers, 2016) reveals an evocative example how users do their own workaround to be careful about potential data security risks from anyone who tries to gain remote access. At the same time, the example also shows us where future product/service designers and engineers should be more cautious to prevent potential data breaches from their created products, making their hardware products more secure and reliable from possible cyber attacks.

5. Discussions

5.1. Reflection on the setting of the design challenge

The aim of our research was to shed light on novice designers' current and intrinsic state of awareness of risks associated with cybersecurity challenges when designing new co-robotic and mobile sensing products. A trade-off was made when designing the course set-up and the designated challenge between the amount of internal vs. external creativity constraints (Onarheim, 2012). We wanted to avoid priming the student too much in order to allow them freedom in conducting their customer research and the design of their products. It was also decided not to specifically include cyber security considerations in the final grading in order to focus on human-centric design.

However, in analogous industry conditions (e.g., product safety) more defined and explicit constraints are present, when designing new products. These could show in the form of official requirements in product specification documents, input and collaboration with data-security employees in the company or national/international regulations. As cybersecurity protocols and regulations are continuously shaping, it will be ever more important to consider these constraints in the future. Therefore in future course set-ups it would be relevant to bring in some of these aspects and thereby not only shed light on the current awareness of the students, but also explore which external constraints would support the process of increasing cybersecurity awareness as well.

5.2. Potential impact

Our aim is to involve broader stakeholders in addressing the cybersecurity challenges intertwined with physical co-robots and other connected IoT sensing devices in advanced ways to build a sustainable eco-system. With this approach, we will gain knowledge on awareness and risk in home co-robot interactions. This will be the backbone of guidelines for targeted future users. Furthermore, we expect to broaden the impact by including future product designers of home co-robots. The results of our research will contribute to not only the cybersecurity community, but also product design and manufacturer communities as we bring blended perspectives into one place. By focusing on both the user and designer, we believe our approach will secure long-term effects. As we look ahead to the future, we envision a bold question of "What is a role of physical form of product/service to enhance data security and in the era of cybersecurity, and how does the engineering curricular look like in that era?"

6. Conclusions

Our exploratory research was aimed at understanding how much novice designers are aware of the risk associated with the cybersecurity throughout the design process: Research-Analysis-Ideate-Build-Communicate. As an experimental phase, we track the design process that novice design student teams in the summer course 2017 offered at UC Berkeley had gone through to see how much they carefully took data vulnerability of their created solutions into account. The results revealed that novice design students did not pay much attention to the data vulnerability of the new solutions that they created, in spite of numerous prompts for them to do so. They also failed to adequately understand potential customer and stakeholder sensitivity to cybersecurity issues in their design process. These observations led to the conclusion that we need to further investigate the trade-offs between ease of use and cybersecurity around new product development and how it varies across different user populations and application areas. Design guidelines and curricular material need to be developed with a focus on two populations: (1) targeted vulnerable users and (2) future product designers to secure long-term effects. The goal is to contribute to not only the cybersecurity community, but also product design, development, and manufacturer communities who are dealing with personalized data manipulation in the creation of personal products and services.

Acknowledgment

The authors would like to thank students who participated in our cybersecurity design challenge in the design thinking class offered by the Jacobs Institute for Design Innovation at UC Berkeley, Summer 2017. This research was partially supported by the CLTC (The Center for Long-term Cybersecurity) seed Grant 2017 at UC Berkeley.

References

Amazon Echo and Alexa (2017), *Amazon Echo and Alexa Devices.* [online] Amazon. Available at: https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b?ie=UTF8&node=9818047011 (accessed 03.12.2018)

Bada, M., Sasse, A. and Nurse, J.R.C. (2014), "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?", *Proceedings of the First International Conference on Cyber Security for Sustainable Society, Vol. 3, Coventry, UK, February 26-27, 2015*, pp. 118-131.

Cerrudo, C. and Apa, L. (2017), *Hacking Robots Before Skynet*. [online] IOActive. Available at: https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf (accessed 03.12.2018)

Choudhury, T., Consolvo, S., Harrison, B., Hightower, J., LaMarca, A. et al. (2008), "The mobile sensing platform: An embedded activity recognition system", *IEEE Pervasive Computing*, Vol. 7 No. 2, pp. 32-41. https://doi.org/10.1109/MPRV.2008.39

Denning, T., Matuszek, C., Koscher, K., Smith, J.R. and Kohno, T. (2009), "A spotlight on security and privacy risks with future household robots: attacks and lessons", *Proceedings of the 11th international conference on Ubiquitous computing (UbiComp '09), Orlando, Florida, September 30 - October 3, 2009*, ACM, New York, pp. 105-114. https://doi.org/10.1145/1620545.1620564

Dunn Cavelty, M. (2014), "Breaking the cybersecurity dilemma: Aligning security needs and removing vulnerabilities", *Science and Engineering Ethics*, Vol. 20 No. 3, pp. 701-715. https://doi.org/10.1007/s11948-014-9551-y

Grose, T.K. (2018), "Cyber School", *Prism*, Vol. 27 No. 5, pp. 26-29.

Hurst, G. (2018), *Ban children from Snapchat, parents told*. [online] The Sunday Times. Available at: https://www.thetimes.co.uk/article/ban-children-from-snapchat-parents-told-xf9p8c6ft (accessed 03.12.2018)

iPatrol (2017) *iPatrol.* [online] Available at: https://www.ipatrol.net/ (accessed 03.12.2018)

Jensen, M.B., Wulvik, A., Kriesi, C., Boe, O., Phillip, A. et al. (2016), "Interactions in a world of intelligent products - a case study of a smart and learning office chair", *Proceedings of the 4th International Conference on Design and Creativity (ICDC 2016), Atlanta, USA, November 2-4, 2016.*

Jibo (2017), *Jibo.* [online] Jibo.com. Available at: https://www.jibo.com/ (accessed 03.12.2018)

Ju, W. and Takayama, L. (2009), "Approachability: How people interpret automatic door movement as gesture", *International Journal of Design*, Vol. 3 No. 2.

Kemp, C.C., Edsinger, A. and Torres-Jara, E. (2007), "Challenges for robot manipulation in human environments [grand challenges of robotics]", *IEEE Robotics & Automation Magazine*, Vol. 14 No. 1, pp. 20-29. https://doi.org/10.1109/MRA.2007.339604

Kumar, K. (2017), *Personal Robots Market to Touch $34,120.3 Million by 2022*. [online] P&S Market Research. Available at: https://globenewswire.com/news-release/2017/07/05/1038878/0/en/Personal-Robots-Market-to-Touch-34-120-3-Million-by-2022-P-S-Market-Research.html (accessed 03.12.2018)

Lee, M.K., Kim, J., Forlizzi, J. and Kiesler, S. (2015), "Personalization revisited: a reflective approach helps people better personalize health services and motivates them to increase physical activity", *Proceedings 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15), Osaka, Japan, September 7-11, 2015*, ACM, New York, pp. 743-754. https://doi.org/10.1145/2750858.2807552

Lomas, N. (2018), *Child health advocates call for Facebook to shutter Messenger Kids app*. [online] Techcrunch.com. Available at: https://techcrunch.com/2018/01/30/child-health-advocates-call-for-facebook-to-shutter-messenger-kids-app/ (accessed 03.12.2018)

Markoff, J. (2017), *That Cool Robot May be a Security Risk*. [online] The New York Times. Available at: https://www.nytimes.com/2017/03/01/technology/that-cool-robot-may-be-a-security-risk.html (accessed 03.12.2018)

Matheny, M. (2016), *CloudPassage Study Finds U.S. Universities Failing in Cybersecurity Education*. [online] CloudPassage. Available at: https://www.cloudpassage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/ (accessed 03.12.2018)

Onarheim, B. (2012), "Creativity from constraints in engineering design: lessons learned at Coloplast", *Journal of Engineering Design*, Vol. 23 No. 4, pp. 323-336. https://doi.org/10.1080/09544828.2011.631904

Public Affairs UC Berkeley (2017), *School of Information Offers New Cybersecurity Degree*. [online] UC Berkeley. Available at: http://news.berkeley.edu/story_jump/school-of-information-offers-new-cybersecurity-degree/?utm_content=social-167s3&utm_medium=social&utm_source=SocialMedia&utm_campaign=SocialPilot (accessed 03.12.2018)

Redmiles, E.M., Kross, S. and Mazurek, M.L. (2017), "Where is the Digital Divide?: A Survey of Security, Privacy, and Socioeconomics", *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17), Denver, USA, May 6-11, 2017,* ACM, New York, pp. 931-936. http://doi.org/10.1145/3025453.3025673

Rogers, K. (2016), *Mark Zuckerberg Covers His Laptop Camera. You Should Consider It, Too*. [online] New York Times. Available at: https://www.nytimes.com/2016/06/23/technology/personaltech/mark-zuckerberg-covers-his-laptop-camera-you-should-consider-it-too.html (accessed 03.12.2018)

Said, C. and Baker, D.R. (2017), *Humanizing cars, sensitizing humans*. [online] San Francisco Chronicle. Available at http://www.sfchronicle.com/news/article/Self-driving-cars-human-car-interactions-12215194.php (accessed 03.12.2018)

Security Magazine (2016), *U.S. Universities Failing in Cybersecurity Education*. [online] Security Magazine. Available at: https://www.securitymagazine.com/articles/87062-us-universities-failing-in-cybersecurity-education (accessed 03.12.2018)

Seifert, D. (2017), *Google Home Mini Review: Chasing Dots*. [online] The Verge. Available at: https://www.theverge.com/2017/10/11/16453788/google-home-mini-smart-speaker-review (accessed 03.12.2018)

Sony Aibo (2017), *Aibo*. [online] Sony. Available at http://www.sony-aibo.com (accessed 03.12.2018)

Tao, M. (2017), *Sony Returns To Robotics Market After 12 Years Away*. [online] Robotics & Automation News. Available at: https://roboticsandautomationnews.com/2017/10/08/sony-returns-to-robotics-market-after-12-years-away/14407/ (accessed 03.12.2018)

theDesignExchange (2017), *theDesignExchange project*. [online] UC Berkeley and MIT. Available at: https://www.thedesignexchange.org (accessed 03.12.2018)

Yang, S., Mok, B.K.J., Sirkin, D., Ive, H.P., Maheshwari, R. et al. (2015), “Experiences developing socially acceptable interactions for a robotic trash barrel”, *Proceedings of 24th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN 2015), Kobe, Japan, August 31 – September 4, 2015,* IEEE, pp. 277-284. https://doi.org/10.1109/ROMAN.2015.7333693

Dr. Euiyoung Kim, Postdoctoral Scholar/Lecturer
University of California, Berkeley, Jacobs Institute for Design Innovation
2530 Ridge Road, 94720 Berkeley, United States of America
Email: euiyoungkim@berkeley.edu