Dots and Boxes as a Portable Game System

(Technical Topic)

Transfer Learning in Smart Home Devices: The Standards and The Ethics of Privacy

(STS Topic)

A Thesis Prospectus

In STS 4500

Presented to

The Faculty of the

School of Engineering and Applied Science

University of Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science in Computer Science and Computer Engineering

By

James Tsai

November 1, 2021

Technical Team Members: Joseph Lee, Boheng Mu, Jacob Taylor, James Tsai

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

MC Forelle, Department of Engineering and Society

Harry Powell, Department of Electrical and Computer Engineering

Introduction

Smart home devices such as Amazon Echo, Google Home, and Ring Alarm have taken the household appliance market by storm. It is projected that by 2023, the smart home industry automation in US homes will be 53.9% (Wonder, 2022), meaning 53.9% of US homes will have at least one of these devices. As smart devices become more prevalent in lower and middle socioeconomic status households, the ethical discussion regarding data collection and invasion of privacy also rises among the smart technology stakeholders. Many find it concerning that home appliances can learn its users' habits and daily routines based on when and how they are used, and where their data is stored. Especially with the network of devices connected to the internet, the amount of data collected in a household, if leaked, poses a serious threat to user privacy. This topic is historically comparative to the data leaks of social media platforms, and the distrust in non-transparent data collection methods that arose as a result. As these smart devices grow increasingly invasive, many users may start to wonder: "Why can these devices collect and share data that is private to me?" Since smart homes just recently grew in popularity, "there are no real consensus standards governing design, manufacture, or performance" of smart home devices, and as for laws and regulations, different agencies have varying views, which results in a lack of consistency and proper legal direction (Embry, 2017).

The technical capstone project is a portable game system designed to play the traditionally pen and paper game Dots and Boxes. To ensure safe, scalable, and portable design choices, extensive research was done on safety, programming, and environmental standards and regulations. Standards provide a foundation for technical systems to be easier to use and less expensive to operate. Following standards in the technical project ensures the design will be practical, manufacturable, and marketable. These standards were set by government

organizations, such as The National Institute of Standards and Technology (NIST) and its sub-institutions. NIST was founded not only for the purpose of ensuring technology was compatible with one another, but also ensuring that commercial sales were balanced and able to compete internationally ("Why You Need Standards," 2022).

From a design standpoint, standards play a vital role in the technical and social aspect of a product. Without standards, not only will the product likely not make it to the market, but social concerns about its usage will also arise, such as privacy concerns about smart home device data collection. The ethics of privacy in smart home devices shape their standards and regulations, which lead to a more secure product design.

Dots and Boxes as a Portable Game System

Dots and Boxes is a turn-based, zero-sum game between two players. It was first theorized in 1981 by a French mathematician and is now enlisted as a chess game for the Computer Olympiad (Liangliang et al., 2019). Despite its simple rules, the game offers a multitude of outcomes and strategies and is now the playground for many artificial intelligence and machine learning researchers. The rules of the game are as follows:

(1) Players take turns drawing lines between dots on a *n* by *m* grid

(2) If a player completes a box, they claim the square and may draw another line until they cannot complete a box.

(3) Player with the most claimed boxes wins

(4) Some adaptation of the game sets a timer for both players, when one timer has reached its end, the remaining blocks will be awarded to the player with time remaining.

This game is far from trivial and stimulates the brain by computationally challenging the players to obtain the greatest number of boxes. There has been a widespread usage of arcade entertainment systems, but unfortunately, there is no noteworthy physical adaptation of this game. The main goal of the technical project is to create a device that allows users to set up a game quickly and not need to track ownership of squares throughout the game, since the complexity of the game increases exponentially with size (Zhuang et al., 2015). To achieve these goals, we recreated this classic game with electronic components where players can focus on the game play with an intuitive interface.

Our version of the dots and boxes will offer players an easy interface to select moves and alleviate the burden of constructing the board or the need to keep track and count the squares. Additionally, in contrast to the complete software version, our adaptation invites players to play face-to-face in person, with a physical interface. The system will contain a light emitting diode (LED) array for display, two sets of joysticks for players' input, two push buttons to confirm players' moves, a 7-segment display as the scoreboard, a microcontroller to control the electrical components, and a software program to determine the logic of the game. The microcontroller will deterministically receive player input from the joystick and the button, then pass it to the software program where the game state will be updated and reflected on the LED array and the scoreboard. The technical project transforms a game that is normally played with paper and pen into a more efficient and autonomous platform, providing a better experience.

There are many standards that act as the foundation for the system design: The PCB design and manufacturing process will follow the standards set by IPC-2221 for general board design (IPC, 1998). The component mounting and interconnection structures will follow the same standards. Components that are housed in the 3D printed frame will be protected from

abrasion, and any openings in the frame will be effectively closed, according to the United States Department of Labor Occupational Safety and Health Administration (OSHA) standard 1910.305(b)(1)(i) (1910.305 - Wiring Methods, Components, and Equipment for General Use. | Occupational Safety and Health Administration, n.d.). Programming the device using embedded C/C++ will follow the Embedded C Coding Standard set by the Barr Group to minimize bugs in firmware and improve the maintainability and portability of embedded software (Barr Group, 2016). If the dots and boxes game were to go into large scale production and used in an amusement venue, it would have to fall under the OSHA Industry Group 7999 standards for Amusement and Recreation Services (Description for 7999: Amusement and Recreation Services, Not Elsewhere Classified | Occupational Safety and Health Administration, n.d.). These standards, along with many more, act as the unifying factor for this game system to integrate seamlessly into the network of pre-existing game technologies, as well as allow users to see the environmental, ethical, and societal impact this system has.

Transfer Learning in Smart Home Devices and Their Ethics of Privacy

To understand the ethics surrounding smart home device privacy, Bruno Latour's Actor Network Theory (ANT) framework will be used to analyze the socio-technical connections between smart home devices, their standards, and their users, as well as each actor's roles in shaping each other's development (Latour, 2007). ANT is an STS framework that views technology and society as relational webs where human and non-human actors are treated equally in the network. These actors are analyzed for their role in constructing technological systems, in this case, how smart home device privacy issues affect their standards and public opinion. However, the context for specific data collection methods for those devices and the

applications of that data should be defined first. Privacy concerns arose from technology experts exposing smart home device data collection methods and spreading word about it on internet forums. Rebecca Herold, CEO of Privacy and Security Brainiacs, highlights a few main problems with smart device security: most devices do not have built-in security or privacy controls to protect sensitive data transmissions, listening on smart devices are turned on by default, online connections can compromise device security, and device manufacturers and vendors have vague privacy notices that give them rights to control user data (Herold, 2020). These concerns affect the security design of smart devices, which include improved encryption and transfer learning (how data learned in one device can be used in another) methods (Yang et al., 2021; Anjomshoaa & Curry, 2021).

ANT will be used to reveal overlooked complexities of technology and black-box them in the connected network to understand how that technology influences the social and vice versa (Cressman, 2009). Key actors in the smart home network are not limited to just the devices and the user; data storage systems and social barriers also influence the design and social views of smart home technology. These actors set the foundation for the balance between privacy, security, and functionality of a smart home device. For the technology to provide value to the consumer, it must obtain and process sensitive data from the consumer, but in turn, the consumer wants to limit privacy invasiveness of the device (Ferraris et al., 2021). This stalemate ultimately constrains the complexity level of services that the smart home can realistically provide (Balta-Ozkan et al., 2013). To ease the stalemate, device standards are established as a major actor in the network of all smart devices. Such standards are influenced through both technical and social factors including centralized data storages and acceptable end user agreements (Daivee, n.d.). These factors delegate roles to the standards, which configure both the technology and the users'

lifestyles. Users and smart home devices are constantly evolving, since the technology was recently introduced to society. This evolution is shaped through the cyclic relationship between users, standards, and the device.

Understanding the overall network relies heavily on applying Steve Woolgar's "Configuring the User" theories to ANT. Configuring the User theories analyze the co-construction of a technology and its relationship with other entities (Woolgar, 1990). In this case, human actors that use smart home devices in various ways can influence the development of new features and standards. Malicious attacks can result in improved software security standards, which in turn changes how attackers approach the security of such devices. Additionally, the current lack of laws and regulations for smart home devices decreases users' trust levels and influences device vendors to establish more transparent security measures. These security measures set the boundaries for the devices' delegations on their users as well as configure users to accommodate constantly updating device software.

Research Question and Methods of Research

How do data collection and transfer learning in smart home appliances influence the ethics of smart home privacy standards? To explore this question, case studies and smart home device policies will be analyzed for cases of privacy breaches, how vendors exploit the lack of standardized policies, and how public opinion is influenced by device design. Potential solutions for improved security measures and data collection methods will also be analyzed. Main case study topics include vulnerability of phone applications and transfer learning in smart home sensors (Arabo et al., 2012). Understanding how compromised smart home devices interact with vulnerable phone applications can establish the foundation for security standards for those

devices and applications. Privacy implications in end user agreements for various smart devices will be thoroughly examined for vague and potentially exploitative rights and restrictions. Such legally binding contracts should be clear and concise for users that have a right to know what data is being collected from them. For potential solutions to these issues, current technical research has developed privacy decision frameworks for improving data collection transparency (Keshavarz & Mohd, 2018). Currently developing smart sensor machine learning models are also becoming increasingly advanced, being able to detect data anomalies (Zainab, 2020). Data collected from smart home device machine learning models will be analyzed to see exactly what types of data are being collected and at what frequency they are collected. Assessing the data will help understand what standards need to be enacted or changed. These methods of research will provide adequate information to understand the complex relationships between users, devices, and standards.

Conclusion

Both the technical project and STS topic focus on the impact standards have on technology and society. For Dots and Boxes, scalability and manufacturability are the main driving forces for its standards. Following industry standard design processes for creating a new product not only improves technical skills, but also instills considerations for product safety, environmental impact, and long-term usage. For transfer learning and data privacy in smart homes, standards serve to establish boundaries for device intrusiveness and ameliorate user privacy concerns. Shedding light on the importance of these standards can potentially improve the existing weak framework for smart home device regulation and impact the future usage of smart home devices in everyday life.

References

Arabo, A., Brown, I., & El-Moussa, F. (2012). Privacy in the age of mobility and smart devices in smart homes. *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, 819–826. https://doi.org/10.1109/SocialCom-PASSAT.2012.108

Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy*, *63*, 363–374. https://doi.org/10.1016/j.enpol.2013.08.043

Barr Group. (2016, May 26). *Embedded c coding standard*. https://barrgroup.com/embedded-systems/books/embedded-c-coding-standard

Cressman, D. (2009). *A brief overview of actor-network theory: Punctualization, heterogeneous engineering & translation*. https://summit.sfu.ca/item/13593

Daivee. (n.d.). Ieee device app end user agreements. *IEEE Brand Experience*. Retrieved October 30, 2022, from https://brand-experience.ieee.org/guidelines/digital/mobileapp-and-responsive-design-guidelines/mobile-apps/end-user-agreements/

Embry, S., & Love, G. (2017). *Smart home technology*. National Association of Home Builders. https://www.nahb.org/advocacy/legal-issues/smart-home-technology

Ferraris, D., Bastos, D., Fernandez-Gago, C., & El-Moussa, F. (2021). A trust model for popular smart home devices. *International Journal of Information Security*, *20*(4), 571–587. https://doi.org/10.1007/s10207-020-00519-2

Five common privacy problems in an era of smart devices. (n.d.). ISACA. Retrieved October 30, 2022, from https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/five-common-privacy-problems-in-an-era-of-smart-devices

Georgiev, D. (2022, November 22). *20 eye-opening smart home statistics to know in 2022*. Techjury. https://techjury.net/blog/smart-home-statistics/

IPC. (1998). *Generic Standard on Printed Board Design*. IPC. https://www.ipc.org/TOC/IPC-2221A.pdf

Keshavarz, M., & Anwar, M. (2018). Towards improving privacy control for smart homes: A privacy decision framework. *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, 1–3. https://doi.org/10.1109/PST.2018.8514198

Latour, B. (2007). *Reassembling the social: An introduction to actor-network-theory* (1. publ. in pbk). Oxford Univ. Press.

Occupational Safety and Health Administration. (n.d.). *Description for 7999: Amusement and recreation services, not elsewhere classified | occupational safety and health administration*. United States Department of Labor. Retrieved October 30, 2022, from https://www.osha.gov/sic-manual/7999

Occupational Safety and Health Administration. (2007). *1910.305—Wiring methods, components, and equipment for general use. | Occupational Safety and Health Administration*. United States Department of Labor. https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.305

Why you need standards. (2022). *NIST*. https://www.nist.gov/feature-stories/why-you-need-standards

Woolgar, S. (1990). Configuring the user: The case of usability trials. *The Sociological Review*, *38*(1_suppl), 58–99. https://doi.org/10.1111/j.1467-954X.1990.tb03349.x

Yang, L., Deng, H., Liu, R. P., Wang, P., Dang, X., Tang, Y. Y., & Li, X. (n.d.). Smart home privacy protection based on the improved lsb information hiding. *International Journal of Pattern Recognition and Artificial Intelligence*, *35*(12). https://doi.org/10.1142/S0218001421600053

Zainab, A., S. Refaat, S., & Bouhali, O. (2020). Ensemble-based spam detection in smart home iot devices time series data using machine learning techniques. *Information*, *11*(7), 344. https://doi.org/10.3390/info11070344

Zhang, L., Zhang, Y., Liu, P., & Guo, L. (2015). The research to construct dots and boxes battle platform in computer game. *The 27th Chinese Control and Decision Conference (2015 CCDC)*, 3749–3753. https://doi.org/10.1109/CCDC.2015.7162578

Zhuang, Y., Li, S., Peters, T. V., & Zhang, C. (2015). Improving Monte-Carlo tree search for dots-and-boxes with a novel board representation and artificial neural networks. *2015 IEEE Conference on Computational Intelligence and Games (CIG)*, 314–321. https://doi.org/10.1109/CIG.2015.7317912