Privacy Interventions and Education (PIE): Encouraging Privacy Protective Behavioral Change Online

Garrett Smith
Brigham Young University
USA

Kirsten Chapman
Brigham Young University
USA

Zainab Agha
Vanderbilt University
USA

Janet Ruppert
University of Colorado Boulder
USA

Spring Cullen
Brigham Young University
USA

Sushmita Khan
Clemson University
USA

Bart Knijnenburg
Clemson University
USA

Jessica Vitak
University of Maryland, College Park
USA

Priya Kumar
Pennsylvania State University
USA

Pamela Wisniewski
Vanderbilt University
USA

Xinru Page
Brigham Young University
USA

ACM Reference Format:
Garrett Smith, Kirsten Chapman, Zainab Agha, Janet Ruppert, Spring Cullen, Sushmita Khan, Bart Knijnenburg, Jessica Vitak, Priya Kumar, Pamela Wisniewski, and Xinru Page. 2023. Privacy Interventions and Education (PIE): Encouraging Privacy Protective Behavioral Change Online. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23), April 23–28, 2023, Hamburg, Germany*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3544549.3573816

1 INTRODUCTION

Networked privacy is a key research topic surrounding many discourses within SIGCHI and adjacent communities, and often needs to be tackled from multiple disciplinary perspectives as well as needing to take into account real world environments, policies, and impact. Being able to bring academics and industry practitioners together to tackle the challenges with online privacy is key to making progress in this area. Previous workshops around online privacy have sparked momentum towards addressing some key areas of privacy research. For instance, identifying the trade-offs between maintaining privacy and managing personal information sharing [31], gaining insights into how to bridge the gap between privacy theory and design [27], uncovering individual variations in privacy attitudes and concerns [24], as well as recognizing elevated privacy risks and consequences faced by vulnerable populations [22, 26]. Recent workshops have also explored evolving privacy needs in newer technical domains, including Artificial Intelligence (AI) [14, 35] and Internet of Things (IoT) technologies [32].

Despite considerable advances in SIGCHI privacy scholarship over the last decade, there remains a challenge that for the most part, people are still privacy concerned and at risk of privacy violations, but not necessarily engaging in beneficial privacy-protective behavior [5, 7, 8]. Building on the foundational conversations of previous privacy workshops that identify key privacy issues and consequences, this workshop aims to take privacy research to the next step. We bring CHI attendees together to take on the particularly difficult challenge of developing effective privacy education that supports users in making sustainable privacy-protective behavioral changes. We must explore both practical and theoretical pathways to advance privacy education scholarship. Furthermore, it is important to recognize that traditionally underrepresented groups (e.g., low-socioeconomic background, LGBTQ+, foster youth, immigrants, older adults) may be either more susceptible to privacy risks online, or more heavily impacted by a given privacy violation, requiring special considerations for effective privacy education and behavior change.

Previously, privacy researchers have investigated these problems primarily from three separate perspectives; privacy education, intelligent systems and interventions, and privacy design. Yet, people are still not engaging in privacy-protective behaviors in many contexts and concerns about online privacy are at an all-time high [5, 7, 8, 25]. Each of these three perspectives focus on an important yet different part of the equation for motivating and enabling privacy protective practices. Thus, we bring these communities together to take a three-pronged approach to privacy-protective behavior change. By doing so, we may be able to develop solutions at the intersection of education, design, and intelligent interventions that more aggressively tackle the several problems associated with enabling and motivating change. Our workshop aims to build a bridge between these different efforts so that we can learn from one another and spark ideas about novel ways to empower end-users to better manage their privacy. We invite privacy scholars and industry practitioners to come together at CHI and build a community that will allow us to work towards effective privacy protecting behavioral change.

CHI EA '23, April 23–28, 2023, Hamburg, Germany
© 2023 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9422-2/23/04.
https://doi.org/10.1145/3544549.3573816

2 BACKGROUND

Here we briefly review the three main areas of work that take different approaches to privacy protecting behavioral change. These strands of research have largely been operating in parallel and we believe bringing them together will allow us to move forward as a research community to address the increasingly prevalent and problematic privacy issues online.

2.1 Privacy Education

Networked privacy education has been studied for different target audiences within the SIGCHI and related communities. Several researchers have focused on theoretical work to measure digital privacy literacy [30], improving awareness about social media privacy controls [28], and educating the general population about online privacy disclosures through teaching curriculum [9]. Recently, some scholars have extended this work to focus on the privacy needs and education of underrepresented groups. For example, Kumar et al. have investigated effective ways to provide online privacy education for children, ranging from interactive games and stories [16], to strengthening childrens' privacy literacy through contextual integrity [18], to integrating privacy lessons into the classroom and home [17]. Similarly, privacy literacy for older adults has also been investigated and compared against other groups [11, 12]. Findings from prior work suggest that existing education practices are often time-consuming [21], inequitable [6], and often fail to bring about behavioral change, sometimes referred to as the privacy paradox [15], as users already have ingrained privacy practices.

2.2 Intelligent User Interfaces and Interventions

In addition to researching ways of delivering privacy education to a broader audience, scholars have more recently investigated potential intelligent user interface (IUI) based intervention methods that empower and encourage users to make privacy-preserving decisions [13, 29, 33]. Examples of scholarly contribution in IUI-based intervention include "nudges" to inform users about their privacy choices [13], personalized intervention to promote privacy-preserving behavior [33], and automation of privacy features [23]. Despite these efforts, many users still struggle to adopt privacy-preserving behavioral practices. Often times privacy instructions and policies are riddled with jargon and complex processes that general users are not familiar with [3]. As a result, deciphering the content can get overwhelming for non-domain experts, dissuading them from learning about privacy best practices. Thus to ensure the adoption of IUI-based interventions, it is imperative that users' have well-rounded privacy knowledge such that they can easily engage with interventions and adopt them.

2.3 Privacy Design

Another group of researchers have focused on developing novel privacy designs that can help improve users' decision-making and privacy experiences online. Some of these efforts have focused on co-designing privacy features that empower the end-user to be involved in the design process, to uniquely cater to their needs. For instance, Ashktorab et al. conducted participatory design sessions with high-school students to design solutions for mitigating online risks [4]. Along similar lines, Agha et al. conducted bootcamps with teens to design real-time online safety and privacy interventions that can provide personalized privacy guidance to teens and educate them towards behavioral change [1].

In parallel, other efforts have focused on designing to support collaborative practices for managing online privacy within families [2], crowd-sourcing approaches to mobile privacy [20], as well as privacy design for IoT devices [34] and Augmented Reality [19]. Strikingly, a common theme that has come out of these recent studies is that privacy design needs to sit at the intersection of intelligent systems and education; relying on intelligent detection of privacy risks and incorporating education as part of the design. Scholars suggest that doing this could make privacy designs much more effective. Thus, we focus on this in our workshop. Additionally, many questions still remain unanswered in the privacy design literature such as when and how should we provide privacy education and encourage privacy protective behavioral change? How can we do this in a way that is ethical and improves privacy decision-making, balancing personalized privacy protection against user autonomy?

3 WORKSHOP DESCRIPTION

Our workshop aims to tackle these questions and challenges by bringing together academic and industry experts to work towards developing actionable recommendations for effective and equitable privacy interventions and education. In additional to the broad goal of cross-pollination of ideas, we also specifically focus on the following **workshop themes**:

- Enumerating potential power imbalances in access or effectiveness of privacy education and interventions that may come as a result of unique individual differences (e.g., culture, age, privacy literacy).
- Identifying educational and learning models (e.g., Bloom's taxonomy [10]) that can inform design for privacy interventions and education.
- Identifying existing research into designing and implementing lightweight persuasive interventions that support privacy decision making, as well as gaps in the current literature.
- Identifying actionable ways to overcome ethical and practical concerns around implementing privacy interventions.

Therefore, this workshop brings together privacy researchers, designers, and experts in order to address these multi-faceted challenges and build a community that will be better able to co-create actionable ways for effective privacy intervention and education. More concretely, in coming together to address the above challenges, this workshop will also make the following contributions to the broader academic community:

- Building a community of researchers passionate about privacy intervention and education that can spark new collaborations and facilitate mentoring for scholars new to the field.
- Establish a baseline of existing knowledge to help scholars understand what has been done and build on that existing literature.
- Provide the research community with a prioritized map of gaps in the literature and list of equity challenges that must be addressed in privacy education and interventions.

To accomplish these goals, we have planned activities to engage workshop participants not only on the day of the workshop, but also offer ways to keep participants connected beforehand and afterwards. We will also run a hybrid workshop to enable involvement by a broader group of researchers. We describe these plans in the remainder of the proposal.

3.1 Pre-Workshop Plans

Participants will connect through a Slack space created for this workshop and community. Through this channel, future communications and workshop updates will be announced to all participants. It will also give workshop attendees an opportunity to introduce themselves, read panelist bios, submit panelist questions for discussion and get access to workshop submission papers to read prior to the day of the workshop. It will also serve as a means to engage during the workshop itself, in particular for those who are participating virtually (details below), and for post-workshop discussions to continue. With authors' permission, we intend to share position papers and other resources to the workshop website prior to the workshop.

3.2 Workshop Mode

We aim to create an inclusive environment for all to participate. Thus, we have planned a hybrid workshop in order to facilitate both in-person and virtual workshop attendance. Virtual attendees will be able to participate in small group conversations with one another over Zoom. At least one workshop organizer will be moderating the Zoom conversations. Both in-person and virtual participants will be encouraged to use the workshop slack to brainstorm and upvote ideas, and engage in discussion around these ideas. During the workshop, activities will take place over collaborative online whiteboard tools such as Google Jamboard and Miro, which participants may view, comment, and edit outside of workshop sessions. Virtual attendees will also be able to participate in the large-group discussion and panels by posting questions to the slack which will be called out by a workshop organizer dedicated to ensuring virtual participants voices are heard. Several of the organizers have experience using Slack for facilitating these types of activities and will be able to draw on their past experience to successfully utilize this tool.

3.3 Workshop Structure

This workshop structure will be as follows.

1. Welcome, Introduction and Lightning Talks (1 hr) Organizers will introduce themselves and discuss the overall plans for the workshop. Each attendee will be given a specified amount of time to present their accepted workshop papers. The amount of time will be dependent on the quantity of submissions accepted.

2. Discussion (1 hr) Attendees will be randomly assigned a small group where they will answer the following questions:

- *What has been found in current research?*
- *What are the gaps in current literature?*
- *What educational/learning models can be applied to privacy?*
- *What contexts would educational interventions be appropriate*

After each question, attendees will come back together as a large group and discuss their small group's findings. Attendees will then be randomly assigned to new groups.

4. Break (15 min) During the break, organizers will use affinity diagramming to determine relevant contexts for the design activity.

5. Panel (1hr 15 min) A panel consisting of industry and academic researchers working at the forefront of privacy education and interventions will answer questions regarding privacy interventions and education. The last author will moderate the panel. The panelists will be:

- **Bart Knijnenburg** Associate Professor, Clemson University
- **Jen Romano** UX Research Lead and Manager at Google
- **Jessica Vitak** Associate Professor, University of Maryland
- **Liz Keneski** Director of Privacy Research at Meta
- **Pamela Wisniewski** Associate Professor, Vanderbilt University
- **Priya Kumar** Assistant Professor, Pennsylvania State University

6. Lunch (1 hr 30 min)

7. Design Activity Round 1 (40 min) Attendees will be divided into small groups and given a context based on the morning discussion. They will be tasked with developing an intervention or educational material related to their assigned context for a general audience. After 30 minutes, small groups will come together to share their designs.

8. Design Activity Round 2 (30 min) Participants will rejoin their small groups to continue with their design, incorporating feedback from the large group. The small groups will then identify and discuss ethical concerns or power imbalances that may exist when applying their design to more specific audiences (i.e., teens, refugees, neuro-diverse, etc.)

9. Design Activity Round 3 (20 min) After identifying these concerns, attendees will then choose one or more populations discussed in round 2 and redesign their intervention or educational material to specifically support this group.

10. Break (15 min)

11. Large Group Reporting and Discussion (30 min) Groups will share their intervention or educational material with all attendees.

12. Concluding Remarks and Where to Go From Here (30 min) Opportunities for continued participation will be discussed. All participants will be invited to participate in a post-workshop write up.

3.4 Post-Workshop Plans

After the workshop, the organizers will compile and publish the takeaways in a blog post or article, posted on the workshop website. We plan to make recordings of main sessions (not breakout room sessions) available to participants, but not to the general public. Design ideas or artifacts created during the workshop activities will also be published on the workshop website for researchers use in future work. Any insights found during the discussions and design activities will be shared with the workshop participants via email, a dedicated Slack channel and through the workshop website. The organizers also plan to include participants in a Slack channel for continuing the discussion around privacy interventions and education after the workshop, focusing on key takeaways and next steps.

3.5 Call for Participation

Recruitment for this workshop will take place through our workshop website at pie.stapl.cs.byu.edu. Organizers will also use social media channels such as the Facebook Groups ACM SIGCHI, CHI Meta, and their own personal networks to recruit attendees. Interested attendees will be able to apply via Google Form. Participants will be able to express interest in two ways: a 2-4 page position paper or a statement of interest. The workshop paper will be in the ACM Master Article Submission Template format and should describe their research in privacy education or intervention, or address one of the themes of the workshops. Participants that do not have research experience in this area can instead submit a 1-page statement of interest that includes their background and interest in workshop themes.

Participants will be selected based on the quality and relevance of their paper submissions, intent to participate, and their prior experience in Privacy/Education/Intervention. Given that we will offer virtual participation, we hope to be inclusive and include newcomers to the field who have strong interest or plan to engage in such research. In-person applicants will be selected in ways that will encourage lively and engaging discussion. We will attempt to assemble a diverse group of participants.

Submissions should be emailed to networkedprivacy2023@gmail.com. Each submissions will be reviewed by 2 PC members. At least one author for each accepted submission must register and attend the workshop and at least one day of the conference.

3.6 PC Members

The following scholars have committed to being on the Program Committee for this workshop if it is accepted.

- **Afsaneh Razi** Drexel University
- **Airi Lampinen** Stockholm University
- **Apu Kapadia** Indiana University
- **Blase Ur** University of Chicago
- **Daniel Zappala** Brigham Young University
- **Daricia Wilkinson** Microsoft Research
- **Jen King** Stanford University
- **Karla Badillo-Urquiola** University of Notre Dame
- **Kent Seamons** Brigham Young University
- **Louise Barkhuus** IT University of Copenhagen
- **Mainack Mondal** Indian Institure of Technology Kharagpur
- **Michael Zimmer** Marquette University
- **Moses Namara** Meta
- **Norah Abokhodair** Microsoft Learning Innovation Studio
- **Oksana Kulyk** IT University of Copenhagen
- **Reza Ghaiumy Anaraky** New York University
- **Smirity Kaushik** University of Illinois at Urbana-Champaign
- **Tanusree Sharma** University of Illinois at Urbana-Champaign
- **Yaxing Yao** University of Maryland, Baltimore

4 ABOUT THE ORGANIZERS

Garrett Smith is a PhD Candidate in Computer Science at Brigham Young University. Broadly speaking, his research seeks to understand privacy issues surrounding social media usage. He is especially focused on using interventions to help people reflect on their privacy behaviors and seeing how that affects their long-term privacy preserving behavior on social media.

Kirsten Chapman is a researcher in the Social Technology and Privacy Lab (STaPL) at Brigham Young University. Her research focuses on making social media more privacy protective for individuals in neurodiverse populations, such as those in the Autism Community, through use of educational interventions. She is working on more effective ways to co-design with the populations she serves.

Zainab Agha is a PhD student in Computer Science at Vanderbilt University. Her research lies at the intersection of adolescent online safety, privacy, and co-design, with a focus on co-designing and evaluating effective online safety interventions for social media with teens.

Janet Ruppert is PhD Candidate in Information Science at the University of Colorado Boulder. Ruppert researches attitudes and hands-on, creative educational interventions in informal learning settings around institutional privacy and surveillance for teenagers.

Spring Cullen is a Master's student at Brigham Young University focusing on understanding how privacy models need to be extended to account for Neurodiversity. She works with young adults on the Autism Spectrum in order to ground her understanding of privacy expectations and violations.

Sushmita Khan is a PhD student at Clemson University. Sushmita researches AI and Privacy education intervention for adolescents.

Bart Knijnenburg is an associate professor in Human Centered Computing at the Clemson University School of Computing. His research focuses on adaptive systems supporting users' privacy decision-making practices. He holds senior and editorial positions for several ACM conferences including CSCW, TheWebConf, IUI, UMAP, RecSys and SOUPS.

Jessica Vitak is an associate professor in the College of Information Studies at the University of Maryland. Her research evaluates the privacy and ethical implications of big data, the internet of things, and other "smart" technologies. She has organized nearly a dozen workshops on networked privacy at CHI, CSCW, and other conferences.

Priya Kumar is an assistant professor at Pennsylvania State University's College of Information Sciences and Technology. She studies discourses related to children's privacy and is developing educational materials to help children strengthen their privacy literacy.

Pamela Wisniewski is an associate professor in the Department of Computer Science at the Vanderbilt University and the Director of the Socio-Technical Interaction Research (STIR) Lab. Her research expertise is situated at the juxtaposition of Social Computing and Privacy with an emphasis on adolescent online safety.

Xinru Page is an associate professor in Computer Science at Brigham Young University. Her research focuses on balancing social connection against privacy concerns on social media, technology adoption and non use, with a particular focus on vulnerable and underserved populations. She has organized many privacy workshops and served in senior editorial and PC roles at conferences such as CHI, CSCW, SOUPS, ICWSM.

REFERENCES

[1] Zainab Agha, Zinan Zhang, Oluwatomisin Obajemu, Luke Shirley, and Pamela J. Wisniewski. 2022. A Case Study on User Experience Bootcamps with Teens to Co-Design Real-Time Online Safety Interventions. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*. 1–8.

[2] Mamtaj Akter, Amy J Godfrey, Jess Kropczynski, Heather R Lipford, and Pamela J Wisniewski. 2022. From Parental Control to Joint Family Oversight: Can Parents and Teens Manage Mobile Online Safety and Privacy as Equals? *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW1 (2022), 1–28.

[3] Reza Ghaiumy Anaraky, David Cherry, and Marie Jarrell. [n. d.]. Testing a comic-based privacy policy.

[4] Zahra Ashktorab and Jessica Vitak. 2016. Designing cyberbullying mitigation and prevention solutions through participatory design with teenagers. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 3895–3905.

[5] BROOKE AUXIER. 2020. *How Americans see digital privacy issues amid the COVID-19 outbreak*. Retrieved Oct 14, 2022 from https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/

[6] Moritz Büchi, Noemi Festic, Natascha Just, and Michael Latzer. 2021. Digital inequalities in online privacy protection: effects of age, education and gender. In *Handbook of digital inequality*. Edward Elgar Publishing, 296–310.

[7] PEW RESEARCH CENTER. 2019. *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Retrieved Oct 14, 2022 from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

[8] Brian X. Chen. 2021. *The Battle for Digital Privacy Is Reshaping the Internet*. Retrieved Oct 14, 2022 from https://www.nytimes.com/2021/09/16/technology/digital-privacy.html

[9] Serge Egelman, Julia Bernd, Gerald Friedland, and Dan Garcia. 2016. The teaching privacy curriculum. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*. 591–596.

[10] Mary Forehand. 2010. Bloom's taxonomy. *Emerging perspectives on learning, teaching, and technology* 41, 4 (2010), 47–56.

[11] Reza Ghaiumy Anaraky, Kaileigh Angela Byrne, Pamela J Wisniewski, Xinru Page, and Bart Knijnenburg. 2021. To disclose or not to disclose: examining the privacy decision-making processes of older vs. younger adults. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–14.

[12] Murat Kezer, Barış Sevi, Zeynep Cemalcilar, and Lemi Baruh. 2016. Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10, 1 (2016).

[13] Bart P Knijnenburg. 2013. Simplifying privacy decisions: Towards interactive and adaptive solutions.. In *Decisions@ RecSys*. Citeseer, 40–41.

[14] Bart P Knijnenburg, Nicole Bannister, and Kelly Caine. [n. d.]. Using Mathematically-Grounded Metaphors to Teach AI-Related Cybersecurity.

[15] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security* 64 (2017), 122–134.

[16] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. 2018. Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th ACM conference on interaction design and children*. 67–79.

[17] Priya C Kumar, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. 2019. Privacy and security considerations for digital technology use in elementary schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[18] Priya C Kumar, Mega Subramaniam, Jessica Vitak, Tamara L Clegg, and Marshini Chetty. 2020. Strengthening children's privacy literacy through contextual integrity. *Media and Communication* 8, 4 (2020), 175–184.

[19] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2018. Towards security and privacy for multi-user augmented reality: Foundations with end users. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 392–408.

[20] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM conference on ubiquitous computing*. 501–510.

[21] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *Isjlp* 4 (2008), 543.

[22] Nora McDonald, Karla Badillo-Urquiola, Morgan G Ames, Nicola Dell, Elizabeth Keneski, Manya Sleeper, and Pamela J Wisniewski. 2020. Privacy and power: Acknowledging the importance of privacy research and design for vulnerable populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–8.

[23] Moses Namara, Henry Sloan, and Bart P Knijnenburg. 2021. The Effectiveness of Adaptation Methods in Improving User Engagement and Privacy Protection on Social Network Sites. (2021).

[24] Xinru Page, Reza Ghaiumy Anaraky, Bart P Knijnenburg, and Pamela J Wisniewski. 2019. Pragmatic tool vs. relational hindrance: Exploring why some social media users avoid privacy features. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–23.

[25] ANDREW PERRIN. 2020. *Half of Americans have decided not to use a product or service because of privacy concerns*. Retrieved Oct 14, 2022 from https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/

[26] Afsaneh Razi, Zainab Agha, Neeraj Chatlani, and Pamela Wisniewski. 2020. Privacy Challenges for Adolescents as a Vulnerable Population. In *Networked Privacy Workshop of the 2020 CHI Conference on Human Factors in Computing Systems*.

[27] Luke Stark, Jen King, Xinru Page, Airi Lampinen, Jessica Vitak, Pamela Wisniewski, Tara Whalen, and Nathaniel Good. 2016. Bridging the gap between privacy by design and privacy in practice. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. 3415–3422.

[28] Alexa Stein, Norman Makoto Su, and Xinru Page. 2020. Learning through Videos: Uncovering Approaches to Educating People about Facebook Privacy. In *Proceedings of the 16th Symposium on Usable Privacy and Security. USENIX.*

[29] Eran Toch, Pamela J Wisniewski, Daricia Wilkinson, Moses Namara, and Karla Badillo-Urquiola. 2018. Moving Beyond A "One-Size Fits All" Approach: Exploring Individual Differences In Privacy. (2018).

[30] Sabine Trepte, Doris Teutsch, Philipp K. Masur, Carolin Eicher, Mona Fischer, Alisa Hennhöfer, and Fabienne Lind. 2015. Do People Know About Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS). In *Reforming European Data Protection Law*, Serge Gutwirth, Ronald Leenes, and Paul de Hert (Eds.). Law, Governance and Technology Series, Vol. 20. Springer Dordrecht, 333–365. https://doi.org/10.1007/978-94-017-9385-8_14 Place: Dordrecht Publisher: Springer Netherlands.

[31] Jessica Vitak, Pamela Wisniewski, Xinru Page, Airi Lampinen, Eden Litt, Ralf De Wolf, Patrick Gage Kelley, and Manya Sleeper. 2015. The future of networked privacy: challenges and opportunities. In *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing*. 267–272.

[32] Jessica Vitak, Michael Zimmer, Anna Lenhart, Sunyup Park, Richmond Y. Wong, and Yaxing Yao. 2021. Designing for Data Awareness: Addressing Privacy and Security Concerns About "Smart" Technologies. In *Companion Publication of the 2021 Conference on Computer Supported Cooperative Work and Social Computing*. 364–367.

[33] Pamela J Wisniewski, Bart P Knijnenburg, and Heather Richter Lipford. 2017. Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of human-computer studies* 98 (2017), 95–108.

[34] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 chi conference on human factors in computing systems*. 1–12.

[35] Tianqing Zhu, Dayong Ye, Wei Wang, Wanlei Zhou, and Philip Yu. 2020. More than privacy: Applying differential privacy in key areas of artificial intelligence. *IEEE Transactions on Knowledge and Data Engineering* (2020).