A Middle-School Case Study: Piloting A Novel Visual Privacy Themed Module for Teaching Societal and Human Security Topics Using Social Media Apps

Ankur Chattopadhyay, David Christian, Adam Ulman and Caleb Sawyer
Department of Information and Computing Sciences
University of Wisconsin - Green Bay
Green Bay, WI, United States
chattopa@uwgb.edu, chridl31@uwgb.edu, ulmaam23@uwgb.edu, sawycm28@uwgb.edu

***Abstract* - This Full paper in the Innovative Practice Category introduces an innovative visual privacy themed pre-university educational module using social media apps for creating privacy awareness as well as teaching societal and human security topics. With the advent of internet (World Wide Web) and social media, and the extensive use of these resources by naïve young users, privacy issues pop up every now and then. The lack of privacy and security awareness may lead to confidential information leaks during the use of online contents, particularly social media. The current IEEE/ACM curricular guidelines in CS, IT and cybersecurity clearly point to a need for inclusion of societal and human security topics at the college level, so that a general awareness can be created regarding today's growing privacy concerns, including privacy issues with media sharing. However, there is still a gap within the K-12 curriculum in regard to these security and privacy topics. Even though there has been some computing educational research work on the topic of data privacy at the K-12 level, the visual privacy theme under the societal and human security domain has hardly been explored within K-12. None of the K-12 cybersecurity educational modules have employed the privacy-enhanced computer vision theme along with a social media platform. This paper intends to address the this gap by presenting a visual privacy themed lesson plan using social media apps for teaching privacy, ethics and machine learning. Its main contribution is a unique visual privacy education based hands-on outreach module that utilizes the PVA (Privacy through Visual Anonymity) notion to teach privacy, ethics and machine learning using media images and videos. Our module uses two freely accessible apps, namely an Obscura Cam and YouTube - Face Blur. These apps are utilized to illustrate the concept of visual privacy and demonstrate PVA in pictures and media clips. Additionally, this paper describes our research case study conducted by piloting our PVA workshop module at the middle-school level. This paper discusses and analyzes the learner data obtained from the workshop participants as part of our Google IgniteCS outreach project. The learning analytics survey data collected during our PVA workshop sessions with various middle-school participants indicate that the described visual privacy module can become a simple yet effective tool for privacy literacy, as it can help build privacy perceptions in young minds. Our acquired results also suggest that that this PVA themed outreach lesson plan can be used as a potential medium for recruiting K-12 students into computing and cybersecurity disciplines.**

Keywords – middle-school; visual privacy; PVA; educational workshop module; social media apps; computing; cyber security; awareness; outreach; societal security; human security; ethics; machine learning; CS; IT; K-12; privacy-enhanced computer vision

I. INTRODUCTION

The recent emphasis on the inclusion of privacy and security topics within the recommended computer science (CS) curricular guidelines [19], latest information technology (IT) curriculum [7, 21] and the new cybersecurity educational guidelines [20] has led many college educators into cybersecurity and privacy themed educational research projects [3, 13, 16]. However, there have been a limited number of curricular building initiatives [3, 4, 5, 8, 11, 12, 15, 22] around privacy and ethics related topics at the pre-university level. Moreover, none of the existing privacy education based K-12 curricular modules [4, 5, 8, 11, 15, 22] focus on the 'visual privacy' theme or PVA concept. Also, none of these modules use computer vision or machine learning to educate youth about realistic media privacy issues that exist in today's digital society. As existing literature [3, 5, 11, 12, 17, 18, 22] suggests, there is a clear need for inclusion of privacy modules, which fall under the societal and human privacy domain [20], at the K-12 level, especially for the middle-school youth. To our knowledge, this proposed visual privacy themed nifty module is the first of its kind at the middle-school level to be based upon the theme of visual privacy or PVA (under the topic of privacy-enhanced computer vision). Very few prior work [3, 12] explore the visual privacy theme in educational curriculum design and development, but they focus primarily on the university level, and not K-12. Our innovative visual privacy themed middle-school lesson plan teaches students the essential concepts of privacy, ethics and machine learning by practical demonstration of PVA [3] in social media images and video clips, using the exclusive Privacy Cam model of privacy through invertible cryptographic obscuration [2].

The fast-growing use of smartphone cameras and other recording devices in public spaces has created mounting concerns about privacy. These concerns are only exacerbated by the advancements in computer vision and machine learning [2]. One might think that the significance of such public issues would lead to increased efforts to spread awareness of privacy in the public surveillance domain, especially at the K-12 level.

978-1-5386-1174-6/18/$31.00 ©2018 IEEE

However, this is not the case, as many K-12 schools lack formal privacy or cyber security topics in their curriculum. When computing topics are taught in K-12, the lessons are often shallow and insufficient content wise [17].This leads to potential gaps and holes in the K-12 curriculum, because understanding societal and human privacy notions is a key aspect of being a digitally literate person [18].

According to the Internet Keep Safe Coalition (iKeepSafe), students should be able to understand why privacy matters, as well as the security tradeoffs that come with privacy [11]. They should also be able to recognize when and how personal information is shared, as well as realize the implications of doing so [12]. In the process of educating K-12 students about privacy issues, we also prepare them for potential entrance into cybersecurity related fields that some reports indicate have a workforce shortage of 20,000 to 30,000 professionals in the US public sector alone [13]. However, even current students, who do choose to study cybersecurity at universities, may face some challenges, as they may not be able to reach mastery in the skills expected by employers in the 3-5 years of their college careers. To remedy this problem, some have suggested that computing education should take an approach similar to K-12 music education i.e. a strategy of facilitating hands on practice and mentorship at an earlier age [14] - a model which our proposed hands-on privacy workshop module could help realize. Thus, this forms the motivational basis of our visual privacy themed middle-school lesson plan.

II. BACKGROUND

With the rise in the usage of online social media via social networking websites [1, 9], and the widespread deployment of public surveillance [3], the issue of privacy invasion looms large in today's visual media contents. The lack of clear understanding about private and public spaces makes today's youth relatively easy targets as naïve users of social media, leading to loss of privacy and confidentiality compromises. On the other hand, with the extensive use of public surveillance cameras, there is a growing debate as to whether the excessive security measures, in relation to public space monitoring, are violating our basic privacy rights [3]. Additionally, there is a rising dilemma amongst the public, especially the youth in today's digital world when it comes to choosing either privacy or security i.e. one over the other. This discussion may lead to public concerns related to the invasion of personal privacy. Participation in such a nationwide debate typically requires a minimal understanding of privacy, ethics, privacy versus security as well as the need for a fine balance between privacy and security [2, 3]. Our youth needs to be made aware of these privacy related topics and ethics at an early age as part of the process of being educated for cybersecurity-based literacy [3, 22]. Thus, the overall requirement of including the above mentioned knowledge elements within the K-12 curriculum motivates the creation of our novel educational privacy workshop module (as discussed in this paper), as it will help in developing privacy awareness.

The above mentioned debate around opting for privacy at the cost of security, or security at the cost of privacy stems around societal privacy concerns, including the places where security has gone too far [2, 3]. The advancements in physical security as well as multimedia technology, and personal privacy infringement issues on social media have led to the creation of a mobile app named ObscuraCam [10] and a YouTube video enhancement feature called YouTube Face-Blur [6]. The above mentioned apps offer the option of visual privacy protection to social media users by obscuring the faces of people in uploaded images and videos. The privacy-enhanced media slips, as seen in Figures 1, 2, 3, and 4 illustrate how the YouTube Face-Blur feature works. The YouTube Face-Blur utility allows people to share their videos while maintaining a level of visual anonymity. It also potentially offers some pedagogical advantages for teaching and engaging students, as well as demonstrating the visual privacy theme based upon PVA, given that YouTube platform is very popular with today's youth, including K-12 students. Research statistics and existing literature [1] indicate that 83% of those born between 1995 and 2012 visit the YouTube website quite frequently on a monthly basis, and approximately 50% of teenagers have cited YouTube as their favorite website.

Fig. 1 Image 1 from a Regular News Video Using YouTube

Fig. 2 The Privacy-Enhanced Version of Figure1 - Image 1 Using the YouTube Face-Blur App

Fig. 3 Image 2 from a Regular News Video Using YouTube

Fig. 4 The Privacy-Enhanced Version of Figure 3 - Image 2 Using the YouTube Face-Blur App

ObscuraCam [10] is a free mobile app that helps to safeguard user privacy by obscuring faces in an image or video, which is shared through social media. It preserves privacy via face detection and obscuration through different privacy-enhancing filters, as shown in Figures 6 and 7. It also offers added flexibility of removing any specific region of a pho to or image, including location tags, hence concealing an identity or. This application also uses machine learning in the form of automatic face detection that primarily drives privacy preservation. Existing literature shows that ObscuraCam has been used for a hands-on university lab module based on the PVA theme [3] because it demonstrates privacy and machine learning together. However, it has never been employed at the pre-university level, particularly at the middle-school level, for educational outreach. Prior work [22] indicates that a privacy education based experiential learning model, which is driven by a data privacy theme, can work for increasing privacy awareness in young children.

III. Project Goals

The goal of our unique visual privacy themed educational module is to introduce pre-university students to societal and human privacy topics, ethics and machine learning as well as expose them to computing and cybersecurity in a simple, entertaining yet engaging hands-on lab oriented lesson plan using social media apps. This K-12 educational research and development project was undertaken as part of our Google IgniteCS outreach program, which is intended towards reaching out to the pre-university students under-represented in technology based computing. The design and development of our unique privacy workshop module is an effort to plug an existing hole in the pre-university curriculum, which is due to the absence of engaging and meaningful visual privacy themed lesson plans.

As we present our experimental case study with the created privacy workshop module, we also attempt to gauge the prospects of our nifty visual privacy themed experiential learning model, which represents our efforts towards exposing middle-school youth to the societal and human security domain. It is our aim to use this proposed module to spark the young minds of middle-school learners and encourage them to further explore security and privacy related topics. Through the use of social media driven apps, we hope to capture the attention and curiosity of pre-university students at an early age, so they are better prepared to handle cybersecurity topics when they graduate and move out into the workforce. Thus, this project's primary aspiration is to increase interest and awareness of privacy, security, ethics and machine learning elements. The secondary goal is to increase the overall interest in the computing discipline and tech careers, including cybersecurity studies. We evaluate our module's prospects in terms of meeting these goals by processing the survey data collected from our workshop participants.

IV. Module Description

A. Lesson Plan

Our workshop module starts with a beginning section that covers an introduction to privacy and machine learning's role in privacy. In the next section, ObscuraCam is introduced and demonstrated, which explains how it works and protects user privacy in pictures using facial detection and obscuration. We use the ObscuraCam mobile app's different blurring and masking filters to demonstrate the concept of machine learning and then explain how this enhances user privacy.

After the introduction and demonstration segments of our lesson plan, the student participants are given an opportunity to experiment with the two main applications, namely ObscuraCam and YouTube Face-Blur, so that they can see and experience first-hand the privacy-enhancements to media images plus video clips. The learners are also given a walkthrough instructions in order to guide them through the steps needed to complete the hands-on activities, involving the two media apps, as shown in Figures 5 and 8. Some of these lab exercises, which we have put together around the ObscuraCam mobile app, are illustrated in Figures 6 and 7.

B. Survey Data Collection

After the guided hands-on exploration of the ObscuraCam mobile app and YouTube's Face-Blur utility, we finally proceed to the last segment of our overall lesson plan where we ask the students to participate in an optional and anonymous survey that asks a number of questions about the offered workshop module. Figure 9 lists a selected set of example questions from our survey. The survey questionnaire has been designed in order to gauge participant interests in the

covered privacy concepts, machine learning topics and computing careers. In the next section, the gathered survey data is illustrated graphically in the form of pie charts, which are then discussed in terms of our module's impact and efficacy.

1. Open *ObscuraCam*.
2. Select 'New Picture' from the menu of options.
3. Take a picture of yourself, or a classmate/neighbor (ask their permission before doing so). Tap the check mark in the bottom-right corner of the screen.
4. Once the picture has been taken, *ObscuraCam* will take some time to process.
5. Now, return to the main menu and select 'New Picture' again. Take a picture of multiple faces.
6. Once finished processing, the app will pixelate and display a white box around every face.

Fig. 5 Sample Instructions from First Part of Module - ObscuraCam App

Fig. 6 Screenshot Images of ObscuraCam - Showing App Features

Additionally, our end of workshop survey concludes with a few questions allowing for participant comments and suggestions, including what the participants liked most and least about our workshop module. We will discuss these student feedback comments and inputs as qualitative data in the next section of the paper.

Fig. 7 Examples of Privacy-Enhancing Image Filters of ObscuraCam

1. Navigate to 'https: //www.YouTube.com'.
2. Log into YouTube with your Adam's State account.
3. Select 'Upload' to the right of the search box, near the top of the screen.
4. Click on 'Select Files to Upload'. A file explorer window should open. Navigate to the location of the video of your choice.
5. Click on 'Video Manager' in the upper-right-hand corner of the screen.
6. Find the video you just uploaded and select 'Edit'. Then, select 'Enhancements' near the top of the screen.
7. Select 'Additional Features' below the video player, on the left of the screen. Then select 'Apply' below the 'Blur All Faces' option.
8. All faces should now be blurred!

Fig. 8 Sample Instructions from Second Part of Module - YouTube App

V. Results

Our experimental research case study, as presented in this paper, is based on piloting our nifty visual privacy module with pre-university students at the middle-school level. As described in the earlier sections of this paper, we were particularly interested in teaching the visual privacy notion in conjunction with the related societal and human security perceptions to the middle-school youth, given the need of

exposing these young minds to these topics at an early age [3, 4, 5, 8, 11, 12, 15, 22]. As part of our Google IgniteCS outreach project, we have conducted two (2) separate visual privacy themed workshop sessions with an overall total number of fifty-three (53) middle-school students as participants within the age group of eleven (11) to thirteen (13) years.

Each of these workshop sessions lasted between one (1) hour and one and a half (1.5) hours. Each session featured our unique visual privacy themed lesson plan. The first workshop session had thirty three (33) fifth (5^{th}) graders as participants, while the second workshop session had 20 students as attendees in a mixed group of fifth (5^{th}) and sixth (6^{th}) graders. Each workshop student was given one computer workstation for participating in the designed hands-on lab exercises. In summary, the participants formed a diverse group of middle-school youth, including underrepresented minorities from different public school districts. The gathered survey data from our workshop participants is illustrated graphically later on in this section in the form of pie charts, each of which is then discussed in terms of our module's impact and efficacy.

A. Quantitative Survey Data Analysis

We received forty eight (48) completed survey responses altogether, and the survey results collected from the first and second workshops are presented in Figures 10 - 17. Survey data gathered from workshop 1 indicate that student interest levels in privacy appear to be high before the workshop, with 60% of those participants rating high interest levels, as seen in Figure 10. However, a noteworthy point in this regard is that the interest levels in privacy seem to have risen after workshop 1, with 71% of students reporting a high interest level, as suggested by Figure 13. This upward trend of increased interest levels in privacy from workshop 1 is consistent with the survey data gathered from the second workshop, as shown in Figures 16 and 17. The survey results from workshop 2 also appear to show a significant increase of 50% in the number of participants reporting a high-level of interest before and after the workshop, as seen in Figures 16 and 17.

Next, the survey data on the reported interest levels in machine learning before the first workshop have an even split between a high interest and low interest with few participants showing a neutral disposition, as implied by Figure 11. After workshop 1, these participants self-reported generally higher interest levels, with a majority moving from low (1-2) to moderate (3) interest levels, as indicated in Figure 14.

Lastly, the survey data gathered on student interests in the computing careers before workshop 1 show that less than half of the participants have a high interest in computing careers, and the remaining students are split close to even between neutral and low interest as seen in between the highest level of interest and lowest level of interest, as seen in Figure 12. The data collected for interest levels in computing careers after workshop 1 show a significant rise of 33% in the highly interested category of students that is very heavily biased towards the high interest levels reaching over 80% after workshop 1, as evident in Figure 15.

1. **Scale 1-5:** How would you rate your interest in privacy before this workshop?
2. **Scale 1-5:** How would you rate your interest in privacy after this workshop?
3. **Scale 1-5:** How would you rate your interest in machine learning before this workshop?
4. **Scale 1-5:** How would you rate your interest in machine learning after this workshop?
5. **Scale 1-5:** Before attending this workshop, how would you rate your overall interest in the computing discipline?
6. **Scale 1-5:** After attending this workshop, how would you rate your overall interest in the computing discipline?
7. **Scale 1-5:** After participating in this workshop, how interested are you in pursuing a career in computing?

Fig. 9 Sample Survey Questions from Our Visual Privacy Workshop

B. Pre and Post Workshop Survey Data Comparisons

To gain a better understanding about the observed trend, a comparison of pre and post workshop mean interest levels have been performed for each surveyed field. Beginning with student interest levels in privacy, the sample population's mean interest level before the workshop 1 is reported at 3.18. After workshop 1, this figure rose to 3.86 - a small but clear increase. This might be attributed to the focus of the chosen mobile apps being the visual privacy theme through obscuration filters. As far as machine learning interest levels are concerned, a similar increase is noted - this time from a before mean of 3.00 to an after mean of 3.79. What is most notable about this change is that the minimum recorded interest level for question 4 is '2', as seen in Figures 11 and 14, which is indicative of a sizeable success on getting uninterested students at least partially interested. Finally, the largest change is observed in the interest levels in pursuing computing careers. Here, a change occurred from a mean interest level of 3.18 to 4.25. Notable once more is a minimum interest level of '2' for question 6, as implied in Figures 12 and 15. Therefore, the area of greatest success according to this study in getting diverse groups of middle school students interested in computing careers as a whole.

C. Qualitative Survey Data: Participant Feedback

In addition to the quantitative survey data collection from participants, our study also recorded student responses to optional survey questions on overall workshop module experience, in the form of qualitative student inputs and feedback. These feedback responses have been recorded in regard to the two additional survey questions: *what the participant liked most about our module* and *what the participant liked least about our module*. For question one, a student commented "*we got to learn about how people blurred*

stuff". Another student commented "*I enjoyed learning about privacy and I thought it was cool*." These are some positive comments from our workshop participants that we found helpful for reflecting upon our success in gaining interests in privacy as well as computing careers. Question two included a slightly negative feedback such as "*we would have liked more time to explore and use the app*", which made us consider the option of extending the current hands-on lab time, as part of our present version of the module, with the two (2) privacy-enhancing media apps.

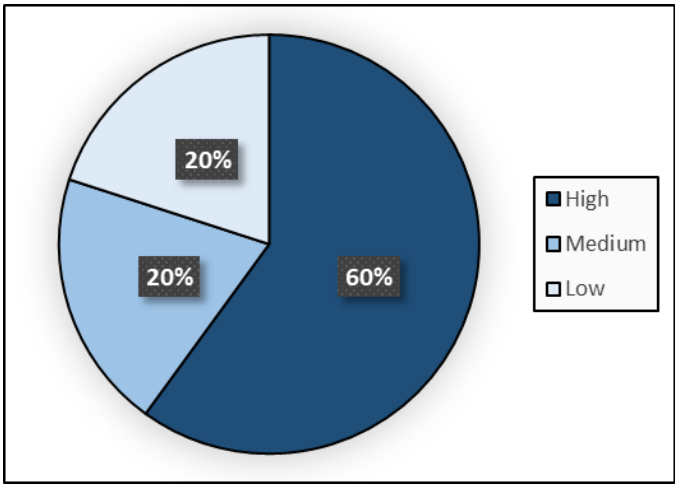

Fig. 10 Student Ratings of Interest Levels in Privacy Before Workshop 1

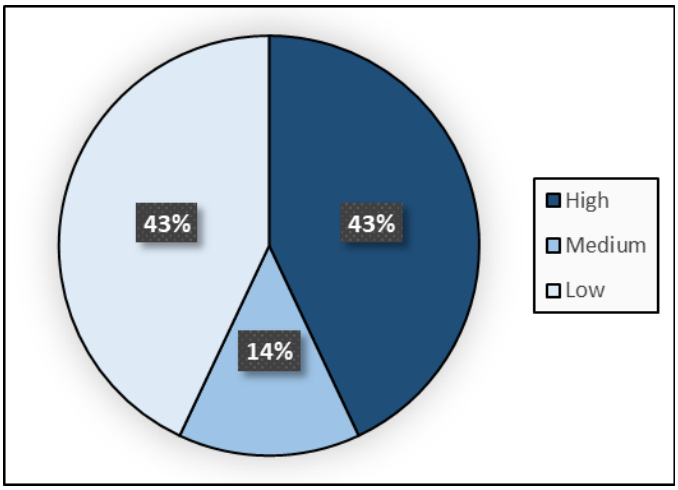

Fig. 11 Student Ratings of Interest Levels in Machine Learning Before Workshop 1

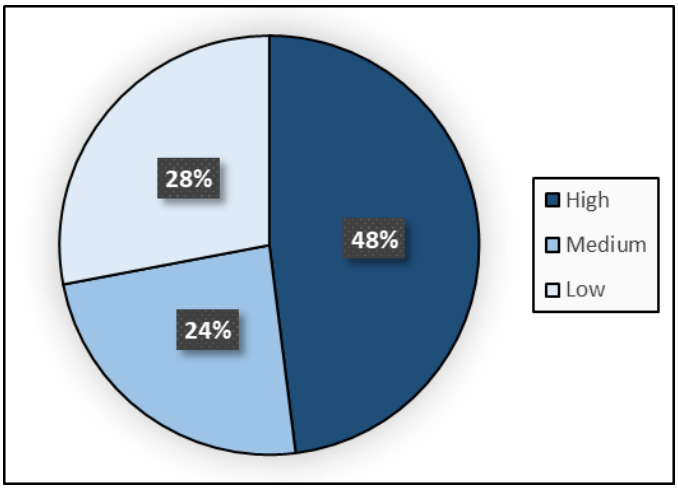

Fig. 12 Student Ratings of Interest Levels in Computing Careers Before Workshop 1

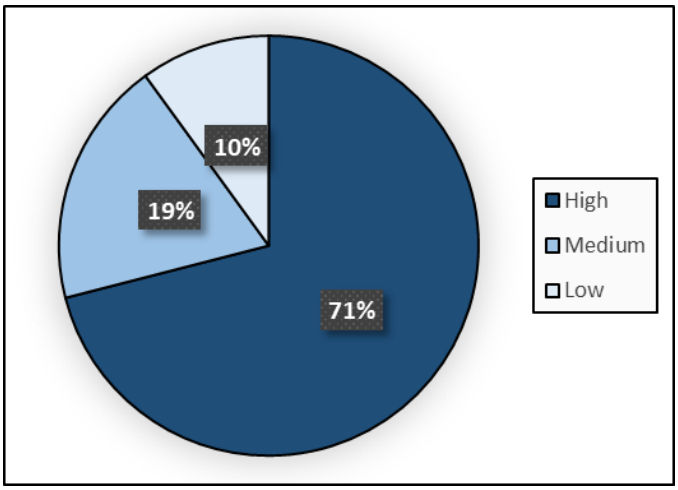

Fig. 13 Student Ratings of Interest Levels in Privacy After Workshop 1

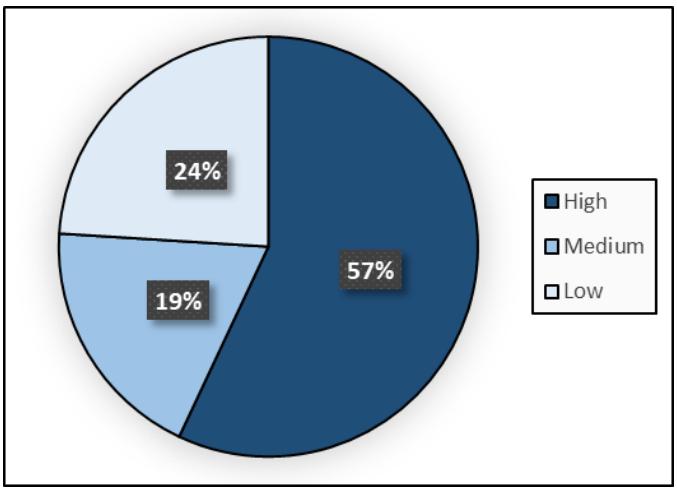

Fig. 14 Student Ratings of Interest Levels in Machine Learning After Workshop 1

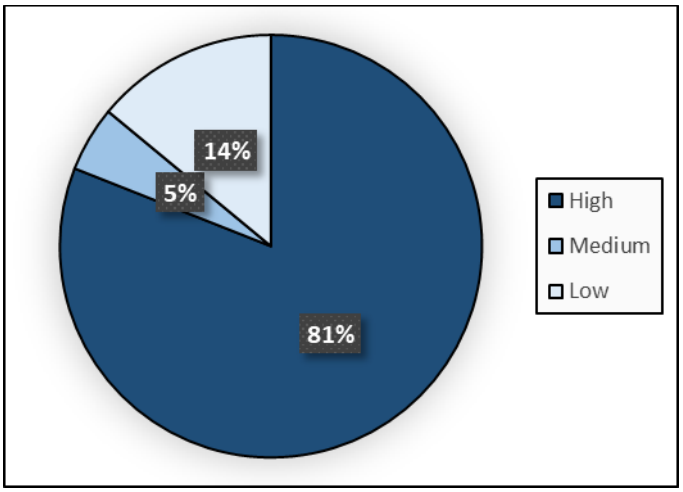

Fig. 15 Student Ratings of Interest Levels in Computing Careers After Workshop 1

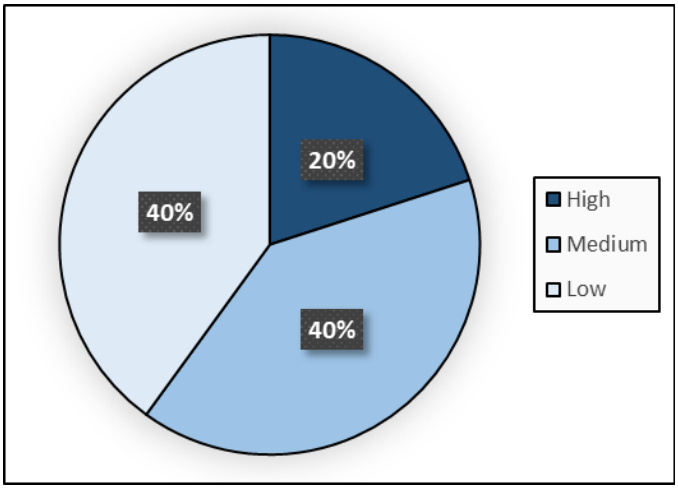

Fig. 16 Student Ratings of Interest Levels in Privacy Before Workshop 2

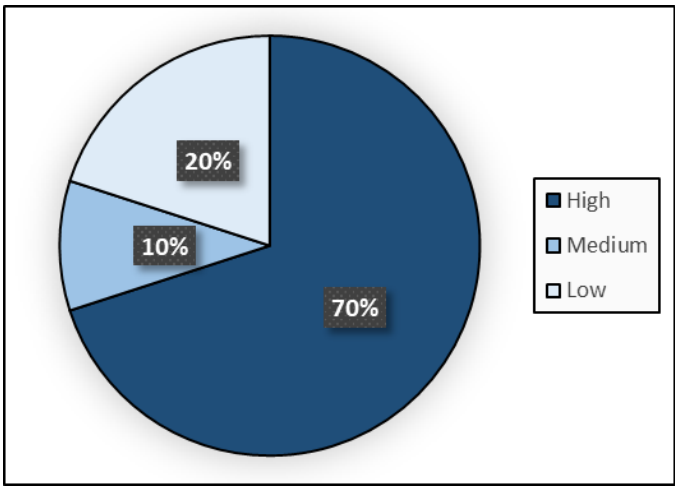

Fig. 17 Student Ratings of Interest Levels in Privacy After Workshop 2

VI. Future Work

As discussed in the previous section, our privacy workshop module has further scope of improvement. One particular limitation of this module is the restricted coverage of cybersecurity topics. The current version of our module only covers societal and human privacy plus security domains. Future work involves expanding the present lesson plan to include usable information security and system security elements, so that students get increased exposure to more cybersecurity concepts, beyond privacy, ethics and machine learning. This may involve building our very own educational tool.

One potential scope of improvement is the extension of the overall lesson plan to include more add-on lesson components, like biometrics, data privacy and trust. These additional lesson components may involve AI and machine learning based hands-on activities as well as networking security based lab exercises.

An additional possible adjustment to our present workshop module is to include some more cybersecurity themed mobile apps and put together some additional hands-on exercises and lab activities around these newly added security apps. This adjustment will help us extend the current lesson plan from one single workshop session to multiple modules for providing the young learners with further exposure to computing and cyber security topics.

VII. Conclusion

This paper introduces our novel visual privacy themed middle-school learning module and presents the corresponding nifty lesson plan, which uses the social media driven apps - ObscuraCam and YouTube Face-Blur to demonstrate and teach privacy, ethics and machine learning. Our lesson plan is carefully designed to create a fun and engaging learning experience in societal and human privacy plus security topics for middle-school youth. It provides a hands on experiential visual learning medium to explore computing and cybersecurity topics. It is meant to create privacy awareness for pre-university students, and encourages them to further explore computing careers, including cybersecurity studies. Through this workshop module, we strive to give middle-school students an early exposure to societal and human privacy plus security related topics, which is essential in today's digital world. Our collected participant survey responses indicate that our lesson plan can become a potential outreach module for recruiting future students in computing and cybersecurity disciplines. It can also contribute towards filling the existing gap of visual privacy themed societal and human security topics at the middle-school level curriculum, so that the young learners get an opportunity to explore computing and cyber topics prior to entering higher education.

Thus, the main goals of this privacy educational module design and development project work is to increase the overall interests in privacy, machine learning as well as the computing and cyber-security disciplines. Our nifty hands-on lesson plan is unique, given it is the first of its kind to focus on the theme of visual privacy (PVA) using computer vision for privacy awareness and computing plus cyber outreach. The survey data that we collected from our pilot workshops strongly point towards the potential of our module in making an impact.

With consistent outreach and continued support from programs like Google IgniteCS, we are hopeful that this initiative would continue to increase privacy and security awareness, as well as succeed in bringing K-12 students into the computing and cybersecurity disciplines.

VIII. Acknowledgements

This visual privacy workshop module design and development project work was supported by Google through their *IgniteCS* program funding. We would like to thank the Google IgniteCS program team for providing us the opportunity to execute this project work, and for sponsoring us to do this pilot research case study.

References

[1] A. E. Barry, E. Johnson, A. Rabre, G. Darville, K. M. Donovan, O. Efunbumi, "Underage Access to Online Alcohol Marketing Content: A YouTube Case Study," *Alcohol and Alcoholism*, Volume 50, Issue 1, 1 January 2015, Pages 89–94. Available at: https://doi.org/10.1093/alcalc/agu078

[2] A. Chattopadhyay and T. E. Boult, "PrivacyCam: a Privacy Preserving Camera Using uCLinux on the Blackfin DSP," *2007 IEEE Conference on Computer Vision and Pattern Recognition*, Minneapolis, MN, 2007, pp. 1-8. Available at: https://doi.org/10.1109/CVPR.2007.383413

[3] A. Chattopadhyay and T. Nehring, "PVA (Privacy Through Visual Anonymity) Lab for Enhancing CS Education and Outreach," *Proceedings of the 45th ACM Technical Symposium on Computer science Education*, March 2014, pp. 723-723. Available at: https://doi.org/10.1145/2538862.2544314

[4] Common Sense Media, Digital Compass. Available at: https://www.commonsensemedia.org/educators/digital-compass

[5] S. Egelman, J. Bernd, G. Friedland, and D. Garcia, "The Teaching Privacy Curriculum," *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, New York, NY, 2014, pp. 591–596. Available at: https://doi.org/10.1145/2839509.2844619

[6] "Face Blurring: When Footage Requires Anonymity." Available at: https://youtube.googleblog.com/2012/07/face-blurring-when-footage-requires.html

[7] "Information Technology Curricula 2017." Available at: http://www.acm.org/binaries/content/assets/education/it2017v085.pdf

[8] AskCypert, K 12 Cyber Security Modules. Available at: http://www.askcypert.org/node/340

[9] J. McFarlane, T. J. McFarlane, and L. Bernard, "Academic Influence of Social Network Sites on the Collegiate Performance of Technical College Students," *World Academy of Science, Engineering and Technology International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, 2017, pp. 1322-332. Available at: scholor.waset.org/1307-6892/10007271

[10] Guardian Project, "ObscuraCam: Secure Smart Camera." Available at: https://guardianproject.info/apps/obscuracam/

[11] Internet Keep Safe Coalition, Privacy K-12 Curriculum Matrix. Available at: http://ikeepsafe.org/privacy-k-12-curriculum-matrix/

[12] D. Rotman, "Are You Looking At Me?," *Social Media and Privacy Literacy*, 2009. Available at: https://www.ideals.illinois.edu/handle/2142/15339

[13] D. C. Rowe, B. M. Lunt, and J. J. Ekstrom, "The Role of Cyber-security in Information Technology Education," *Proceedings of the 2011 Conference on Information Technology Education*, New York, NY, 2011, pp. 113–122. Available at: https://doi.org/10.1145/2047594.2047628

[14] H. Said, "Rethinking IT Education: Lessons from Music Education," *ACM Inroads*, Volume 7, Number 1, March 2016, pp. 34–37. Available at: https://doi.org/10.1145/2838737

[15] International Computer Science Institute, and University of California – Berkeley, *Teaching Privacy*. Available at: http://teachingprivacy.org/

[16] C. F. Turner, B. Taylor, and S. Kaza, "Security in Computer Literacy: A Model for Design, Dissemination, and Assessment," *Proceedings of the 42Nd ACM Technical Symposium on Computer Science Education*, New York, NY, 2011, pp. 15–20. Available at: https://doi.org/10.1145/1953163.1953174

[17] C. Wilson, L. A. Sudol, C. Stephenson, and M. Stehlik, "Running on Empty: The Failure to Teach K-12 Computer Science in the Digital Age," *Communications of the ACM*, Volume 55, Issue 10, 2012. Available at: https://doi.org/10.1145/2347736.2347743

[18] M. Visser, Digital Literacy Definition. ALA Connect, September 2012. Available at: http://connect.ala.org/node/18119

[19] S. Roach, and M. Sahami, "Computer Science Curricula 2013," *Computer*, Volume 48, Issue 3, March 2015, pp. 114-116. Available at: https://doi.org/10.1109/MC.2015.68

[20] Joint Task Force on Cybersecurity Education, "Cybersecuirty Curricula 2017," *Computing Curricula*, Version 1.0, December 2017. Available at: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

[21] M. Sabin, H. Alrumaih, J. Impagliazzo, B. M. Lunt, C. Tang, and M. Zhang, "ACM/IEEE-CS Information Technology Curriculum 2017: A Status Update," *Proceedings of the 16th Annual Conference on Information Technology Education*, Chicago, IL, 2015, pp. 75-76. Available at: https://doi.org/10.1145/2808006.2808013

[22] L. Zhang-Kennedy, K. Baig, and S. Chiasson, "Engaging Children About Online Privacy Through Storytelling in an Interactive Comic," *Proceedings of the 31st British Computer Society Human Computer Interaction Conference*, Sunderland, UK, 2017, pp. 45:1-45:11. Available at: https://doi.org/10.14236/ewic/HCI2017.45