The Teaching Privacy Curriculum

Serge Egelman[1,2], Julia Bernd[1], Gerald Friedland[1], and Dan Garcia[2]
[1]International Computer Science Institute, Berkeley, CA, USA
{egelman,jbernd,fractor}@icsi.berkeley.edu
[2]University of California, Berkeley, CA, USA
{egelman,ddgarcia}@cs.berkeley.edu

ABSTRACT

A basic understanding of online privacy is essential to being an informed digital citizen, and therefore basic privacy education is becoming ever more necessary. Recently released high school and college computer science curricula acknowledge the significantly increased importance of fundamental knowledge about privacy, but do not yet provide concrete content in the area. To address this need, over the past two years, we have developed the Teaching Privacy Project (TPP) curriculum, http://teachingprivacy.org, which educates the general public about online privacy issues. We performed a pilot of our curriculum in a university course for non-CS majors and found that it was effective: weeks after last being exposed, students' privacy attitudes had shifted. In this paper, we describe our curriculum, our evaluation of it in the classroom, and our vision for future privacy education.

CCS Concepts

•Security and privacy → Human and societal aspects of security and privacy; •Applied computing → Education;

1. INTRODUCTION

Despite heightened attention to privacy issues in the popular media, accounts abound of people oversharing personal information online, with sometimes drastic consequences. These stories demonstrate that people still do not have a very good handle on what the specific problems are in sharing information, nor on the steps they can take to manage their privacy. We believe that in this day and age, a basic understanding of online privacy is key to both good cybersecurity practices and to becoming a good digital citizen.

Current computer science curricula aimed at high school and undergraduate students (e.g., the ACM's CS2013 [16] and AP CS:Principles [2]) acknowledge the importance of privacy education, but do not provide content or specific lesson plans. During outreach efforts stemming from our privacy research, many high school and college teachers have told us that they are eager to provide their students with guidance on online privacy, but feel unqualified to do so. In fact, a survey of 12-17 year olds found that 70% had sought outside advice on managing online privacy [11]. To fill this need, we began developing an online privacy curriculum to aid teachers in being able to offer their students actionable advice on how to better protect their personal privacy online. The *Teaching Privacy Project* (TPP) is a privacy education curriculum centered around ten principles and offers students descriptions of how they may be putting themselves at risk online, current threats to personal privacy, interactive demonstrations that illustrate the concepts, and guidance on what they can do to protect themselves.

Our online privacy curriculum is targeted at lay audiences, including high school and undergraduate students (i.e., non-computer science majors), and is accessible to the general public via our website, http://teachingprivacy.org. It is designed to not just convey comprehensive information about current threats to privacy, but to also empower students to do something about it. Rather than taking a prescriptive approach—telling our audience what services they should or should not use—our goal is to provide students with enough information so that they can make their own informed choices about their online privacy. We have been integrating and evaluating parts of TPP in our university's introduction to computer science for non-majors (CS10), which is one of a handful of university pilots of the AP CS:Principles class. CS10 is also the basis for professional development with wide participation from high school teachers. The integration of the TPP curriculum into CS10 has enabled teachers to feel more comfortable about teaching privacy concepts in their high school classrooms, as well as allowed us to receive feedback and improve our curriculum.

To have even broader impact on teachers, we are developing the Teachers' Resources for Online Privacy Education (TROPE), which is based on the TPP curriculum. In the TROPE project, we are building an online teachers' toolkit consisting of classroom-ready teaching modules that educators can use to teach young people about *why* and *how* to protect their privacy online. This way, teachers can easily integrate our curriculum into their classrooms, using as many of our explanatory videos, slide decks, classroom activities, discussion guides, and evaluation materials as they see fit. TROPE also features supporting materials for teachers with background information and guidance on how to employ the modules in the classroom. Our goal is to empower

SIGCSE '16, March 02 - 05, 2016, Memphis, TN, USA

ISBN 978-1-4503-3685-7/16/03…$15.00

DOI: http://dx.doi.org/10.1145/2839509.2844619

teachers to provide students with an understanding of some basic technical and social principles underlying how online privacy works, knowledge of effective techniques they can use to protect their privacy, and the motivation to use those techniques when interacting online.

In this paper, we provide an overview of other privacy education efforts (Section 2) and show that our curriculum is unique in its comprehensiveness and applicability to general audiences. In Section 3, we provide an overview of our curriculum and the teachers' toolkit. In Section 4, we describe our experiences teaching our curriculum in the classroom. Finally, we discuss future work to broaden our curriculum, improve our evaluation metrics, and widen our audience.

2. RELATED WORK

There are a number of existing providers that offer some classroom materials on online privacy, but none offer a comprehensive curriculum *per se*. Common Sense Media's *Digital Citizenship Curriculum* [6] includes among its offerings some privacy-related resources for elementary, middle-school, and high-school classrooms, such as videos and posters and lesson plans on oversharing, identity theft, and privacy policies. Fordham Law School's Center on Law and Information Policy has developed several middle-school lesson plans on privacy that include material on the relationship between security and privacy and the relationship between privacy and reputation management [5]. At the college level, Santa Clara University's *Your Privacy Online* resources cover privacy threats and privacy management from a law and ethics standpoint [13].

These materials are all of high quality—and, in fact, we include links to them on the teachingprivacy.org website—but they do not offer the combination of technical depth, comprehensive coverage of online privacy issues, and focus on U.S.-specific issues and high-school computer-science curriculum standards that we do. Interestingly, some of the most comprehensive efforts have come from Canada and the European Union, such as the privacy lesson plans from Media Smarts [14] (funded by the Privacy Commissioner of Canada) and Teachtoday [19] (funded by Deutsche Telekom).

The resources mentioned above come closest to the Teaching Privacy offerings in quality, scope, and technical grounding, but there are a few others worth noting simply because they are well-known, such as the NetSmartz [8] and Stay Safe Online [1] online-safety classroom materials, which provide some (relatively shallow) coverage of privacy. Several general providers of curriculum content also include some one-off lessons about one aspect of online privacy or another, but are not comprehensive.

In an attempt to locate online privacy curricula aimed at broad audiences, we also examined Massive Open Online Courses (MOOCs). We reviewed existing major providers of high-quality English-language MOOCs (e.g., Coursera, edX, Khan Academy, and Udacity), major universities that provide MOOCs on their own platforms (e.g., Stanford Online and UCLA), and a number of smaller providers (e.g., iversity, Udemy, and OpenLearn). There are several courses that cover privacy from legal, ethical, and policy perspectives (e.g., [20]), or that touch on privacy as it relates to best practices for technology designers (e.g., [18]) and professionals who handle private data (for example, in healthcare) or to cybersecurity and counterterrorism. However, to our knowledge, none offer courses to help non-experts understand the fundamental principles of managing online privacy. While edX and Coursera's introductory computer science offerings and Stanford Online's CS 101 [17] include discussions of Internet structure and cover some security topics, they do not include significant privacy content. In fact, among major providers, the content most similar to ours is edX's new BJCx [9]—which is led by Teaching Privacy's faculty consultant Dr. Dan Garcia and contains some of the Teaching Privacy content. But again, privacy is one topic among many, not the primary focus of the course.

In sum, we believe that our curriculum is unique in combining comprehensive coverage, alignment with U.S. curriculum standards, professional production quality, being accessible to a broad demographic, and grounding in technical expertise. In the next section, we describe the content of our curriculum.

3. THE CURRICULUM

The *Teaching Privacy Project* (TPP) started as an NSF education supplement to develop a set of interactive learning tools to help educators demonstrate what happens to personal information online, and the possible effects of sharing it. To provide context for the demonstrations that we developed, we identified *Ten Principles for Online Privacy* that describe at a high level how online privacy works, technically and socially. These principles form the basis of the TPP curriculum; each principle features an explanation of what it means, why it is important, relevant examples and demonstrations, as well as guidance on how certain privacy threats can be mitigated or outright avoided. The ten principles are as follows:

1. **You're Leaving Footprints**:
   Description: Your information footprint is not just what you intentionally post online. It consists of all of the information that you post or that others post about you, the hidden data attached to those posts by the services you use, the record of your online activities, and also the inferences that can be drawn from putting that collective information together.
   Guidance: Periodically check your privacy settings and update them to limit unintentional sharing.

2. **There's No Anonymity**:
   Description: Your information footprint on the Internet is like your body in the physical world: it defines your identity. Like seeing some part of your body, seeing some part of your information footprint – like the location of the device you're posting from or the pattern of your language – may allow someone to uniquely identify you, even when there is no name or other explicit identifier attached.
   Guidance: Don't do anything online that you wouldn't do in public.

3. **Information Is Valuable**:
   Description: Every piece of information, public or not, has value to somebody: to other people, to companies and organizations, or to governments. They will use your information however benefits them, which may be contrary to your interests—and possibly even embarrassing or dangerous to you.
   Guidance: If you're not sure how your information will be used, don't share it.

4. **Someone Could Listen**:
   Description: Unencrypted communication over the Internet works a lot like sending a postcard: it can be read by anybody along its route. Communication is routed through intermediary computers and systems, which are connected to many more computers and systems. Encryption, or encoding information so it appears scrambled to anyone who doesn't know the key, is a way to wrap a postcard in an envelope. While it can never be 100% secure, stronger encryption makes it harder for people to get to the contents.
   Guidance: Use strong passwords and only communicate sensitive information over secure channels.

5. **Sharing Releases Control**:
   Description: Any time you interact online, that information is recorded. As with in-person communication, once you've shared something, you can't control what happens to it – or how people will interpret it. Other people can repost or forward content to any audience without your permission, websites can sell information to other businesses, and data can be legally subpoenaed. Websites and search engines automatically pick up and duplicate content, making it impossible to "unshare" – the Internet never forgets!
   Guidance: Think before sharing online; ask yourself if you'd be comfortable becoming famous for it.

6. **Search Is Improving**:
   Description: Every day, more data is being put online. Search engines are getting better, allowing "deeper" searching of more types of data. Techniques for extracting and connecting information from different sources are getting more powerful. Furthermore, information that is not retrievable today may be retrievable tomorrow due to changes in terms of service, public policy, or privacy settings.
   Guidance: Monitor your information footprint.

7. **Online Is Real**:
   Description: Your online activities are as much a part of your life as your offline activities; they are interconnected and can affect your life and relationships in the same way.
   Guidance: Share online as if everyone could see it, and would interpret it in the worst possible way.

8. **Identity Isn't Guaranteed**:
   Description: Creating an identity on the Internet or impersonating somebody else is often just a matter of a few clicks. Currently, there is no foolproof way to match a real person with their online identity. This means that you can never be sure with whom you are communicating, and that someone could steal your online identity and impersonate you!
   Guidance: Before you share any information online, consider what you would be risking if the other party wasn't who you thought they were.

9. **You Can't Escape**:
   Description: Even if you're not actively using the Internet, someone else may be sharing information about you – intentionally or unintentionally. So, avoiding the Internet does not guarantee privacy.
   Guidance: Share what you've learned with your friends and family – it will improve your own privacy.

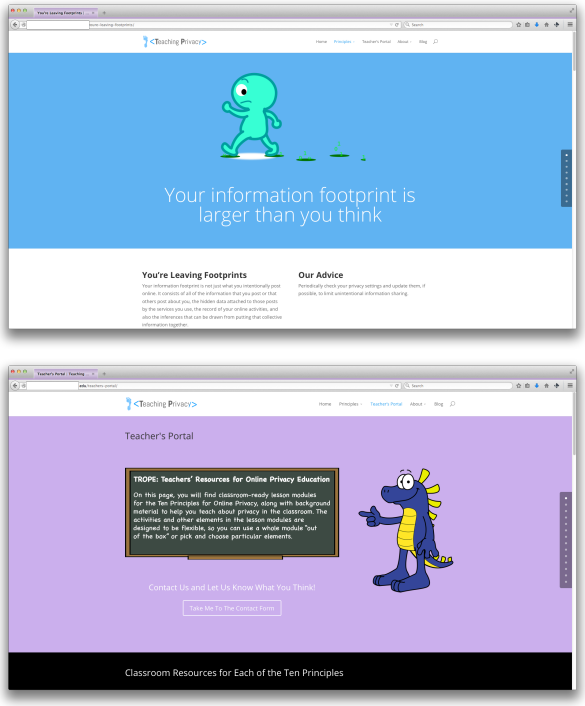

Figure 1: From the TPP website: (a) the principle "You're Leaving Footprints" (b) the Teachers' Portal.

10. **Privacy Requires Work**:
    Description: Most Internet technology is not designed to protect the privacy of those who use it; in fact, most technology providers make money by leveraging your private information. "Privacy policies" are generally written to protect providers from lawsuits, not to protect users' privacy. Laws and regulations cover only certain aspects of privacy and vary from place to place. So, like it or not, your privacy is your own responsibility, and requires your constant attention.
    Guidance: Encourage policymakers to develop comprehensive privacy regulations, educate yourself and others, and be proactive about protecting your privacy.

Taken as a whole, the principles demonstrate the general types of threats to privacy, how they occur, why organizations may exploit them, what the possible consequences are, and what people can do about it. The Teaching Privacy website, http://teachingprivacy.org/, features a separate page for each principle (Figure 1). Each page includes an easy-to-understand description of the underlying concepts; suggestions for actions people can take; questions that prompt broader thinking about the topic; and links to related resources. The principles are accompanied by reinforcing stories and interactive demonstrations. For instance, the *Ready or Not?* app illustrates the principle "You're leaving footprints." It allows a Twitter or Instagram username to be entered, and then shows a heat map and timeline of where and when that user recently posted, based on the geolocation metadata attached to their posts.

We are using this youth-oriented content as the basis for developing a teachers' portal, wherein high school, middle school, and college instructors can download classroom-

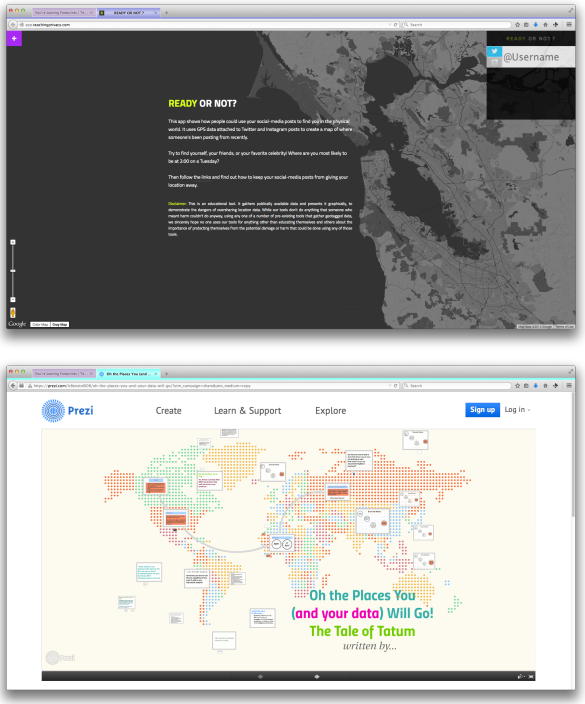

Figure 2: Two of the TROPE lesson elements: (a) the *Ready or Not?* app; (b) the *Oh the Places...* choose-your-own adventure class activity (draft).

ready learning modules and a teachers' guide. Our goal is to make our curriculum available *à la carte* so that teachers can integrate our materials into their lesson plans as they see fit. This effort, the Teachers' Resources for Online Privacy Education (TROPE), was also funded by NSF. It aims to provide teachers with the resources to teach young people about *why* and *how* to protect their privacy online. Each of the TROPE teaching modules is centered around one of the *Ten Principles for Online Privacy* and includes flexible lesson elements that can be used "out of the box" or adapted to supplement teachers' existing lesson materials. These elements include explanations (as slide decks and videos), discussion questions, classroom activities, homework assignments, quizzes, interactive demonstrations (Figure 2), and a glossary of terms. Each module is structured around the 5E constructivist learning model for lesson planning [3]:

- Engagement: Teachers pique students' interest in the topic by asking a question or telling a story to which students can relate.
- Exploration: Students play small-group games or perform exercises in which they explore the technical and social factors that underlie the principle(s), such as activities built around the interactive apps on the Teaching Privacy website.
- Explanation: Teachers use provided slide decks, written materials, and 5- to 10-minute high-quality videos explaining important concepts and effective protection techniques.
- Elaboration: Teachers can use additional discussion questions to encourage students to think about their online behavior; presentation content aimed at translating awareness into action; and suggested group activities or mini-projects.
- Evaluation: We provide assessment tools and follow-up questions so that teachers can measure student learning and we can receive feedback from teachers about the curriculum.

We are also developing supporting materials, including a teachers' guide that provides suggested lesson plans, as well as additional background information. In the future, we hope to develop additional online courseware, such as a Massive Open Online Course (MOOC) based around the TPP curriculum, to help teachers become familiar enough with our curriculum by first completing it themselves. Our goal is to ensure that teachers are comfortable with our content prior to using it in their classrooms.

All of the TROPE materials are released under a Creative Commons license and are being made available via a Teachers' Portal on http://teachingprivacy.org, where we also plan to implement a discussion forum to solicit teacher feedback and answer questions.

4. DISSEMINATION AND EVALUATION

The TPP curriculum and initial TROPE materials are currently being piloted and evaluated through CS10, UC Berkeley's introductory computer science course for non-majors. The course aims to increase the engagement of non-computer-science majors with technological concepts. CS10 is one of only a handful of university pilots for the Advanced Placement *CS:Principles* class (e.g., [10, 2]), and a prolific provider of professional development to high school teachers (with more than 175 teachers in the course's Piazza forum), so the Teaching Privacy Project curriculum is already influencing high schools at a national level. CS10 also has the distinction of being the only computer science course on campus with equal gender representation.

In this section, we discuss how we evaluated our curriculum by measuring its impact on students' privacy attitudes. We describe our method and results.

4.1 Methodology

During the Fall 2014 session of CS10, we piloted elements of the TPP curriculum and examined if they had an effect on students' privacy attitudes at the end of the course. Our hypothesis was that if our curriculum was effective, students would express stronger desires to exert control over their personal information. To test this hypothesis, we asked students to complete a privacy attitudinal scale before and after being exposed to our materials. During the first week of class, and after receiving IRB approval, we emailed the 309 students who were enrolled and asked them to complete an online survey. This initial survey provided a baseline metric of their privacy attitudes. During the final week of classes (week 14), we emailed students to ask them to complete a followup survey. The pre- and post- surveys were identical; the purpose was to observe whether any of their responses had changed over the course of the semester, after being exposed to our materials. Our privacy materials were presented to students during weeks 9 and 11, which means

that by the time that they completed the post-survey, three weeks had passed since they had last been exposed to our materials in the classroom.

Our surveys consisted of a privacy attitudinal scale and an unrelated psychometric scale that is known to exhibit high internal reliability (as measured by Cronbach's α). For the privacy attitudinal scale, we created a hybrid scale by combining Malhotra et al.'s Internet Users Information Privacy Concerns (IUIPC) scale [12] with Buchanan et al.'s Privacy Concerns Scale (PCS), while removing redundant factors as determined by a previous study by Egelman and Peer [7]. This left us with 16 statements that participants rated using a 7-point Likert scale (from "strongly disagree" to "strongly agree"), which were grouped into four sub-scales (Appendix A): concerns about online fraud, online disclosure to companies, transparency and control, and dissemination by others.

Participants also completed the Need for Cognition (NFC) scale [4], which is a well-studied scale in the psychology literature that measures individuals' propensities to engage in "thoughtful" endeavors. We included this scale because it has been observed to have extremely high internal reliability, as measured by Cronbach's α (i.e., $\alpha > 0.8$), as well as remain relatively stable over time. We used the NFC scale as a reliability check for our other responses. Thus, if we observed low internal reliability amongst our sample or a statistically significant change, this would suggest that the responses to both scales are highly questionable and should be discarded (e.g., participants may not have been paying attention and made random selections).

4.2 Results

Of the 309 students enrolled in the class, 260 completed the pre-survey and 201 completed the post-survey. Because our IRB protocol did not allow us to collect personal identifiers, we asked participants to enter the last 5 digits of their university ID numbers so that we could link the pre- and post-surveys. Due to several participants omitting this step or entering non-matching numbers, we were only able to link 119 pre- and post-surveys. Thus, we consider our total response rate to be 38.5%, which we consider to be reasonably good for a voluntary survey with no incentives. Of our 119 participants, 64 were female (53.7% of 119), which did not observably differ from the gender balance of the entire class. Because this was an undergraduate population, we did not examine other demographic traits beyond gender (i.e., participants were likely to fall within the 18-22 age range and were unlikely to hold college degrees).

Based on the reliability of participants' NFC scores ($\alpha_{pre} = 0.86$ and $\alpha_{post} = 0.84$), our data suggests that participants were consistent and took the surveys seriously. We observed no statistically significant change in participants' NFC scores, as measured by a two-tailed Wilcoxon Signed-Ranks test ($\mu_{pre} = 3.52$, $\mu_{post} = 3.50$, $p < 0.826$).[1]

Examining participants' privacy scale responses, we did observe a statistically significant increase, as well as high internal reliability. Averaged across all four sub-scales, participants' scores increased from 5.17 (out of 7) to 5.34 ($\sigma_{pre} = 0.89$, $\sigma_{post} = 0.98$), which was statistically significant ($p < 0.021$). Thus, our hypothesis is supported, and the effect size is between small and medium ($r = 0.21$). Based on this result, we performed post-hoc testing to examine whether this effect was more prominent among any particular sub-scales. Across all four sub-scales, the only statistically significant difference was observed across the "Transparency and Control" sub-scale ($p < 0.003$), which remains significant after correcting for multiple testing, and exhibits a medium effect size ($r = 0.27$). Thus, our results suggest that after completing our curriculum, students exhibited a stronger desire to exert control over their personal information and for more transparency regarding how their information is used by others. This may suggest an increased desire to understand the contents of website privacy policies and/or control if and when companies send them marketing communications.

[1]Unless otherwise noted, we used the Wilcoxon Signed-Ranks test for all within-subjects comparisons in the remainder of this section.

5. DISCUSSION AND FUTURE WORK

Among university undergraduates, our curriculum appears to be effective. Our results show that three weeks after being exposed to our privacy education curriculum, students' attitudes about online privacy had remained changed: they stated an increased desire to have transparency and control over how their personal information is used. However, our work is far from complete. We are actively improving our website and increasing the amount of content that we provide to other educators through our Teachers' Resource for Online Privacy Education (TROPE). Eventually, we hope to develop a full-fledged MOOC so that we can reach much larger audiences of both students and teachers.

One limitation of our work, which applies to both the curriculum itself and the evaluation methodology that we discussed in Section 4, is that it is primarily geared towards those in high school and beyond. For instance, most middle school students (or those even younger) are unlikely to have privacy concerns surrounding business transactions! Yet, these students still experience issues relating to online privacy, just in different ways (e.g., social media usage). We recognize this need and are starting to develop a version of our curriculum that is applicable to a younger demographic, as well as more suitable evaluation metrics.

In addition to directly evaluating our materials in the classroom, we have also hosted several events, including a very popular interactive lab at our university's open house. We also conducted a privacy education workshop at the 2015 ACM SIGCSE conference, and this past summer, our university's NSA/NSF-funded GenCyber summer camp for K-12 students integrated our materials [15]. In addition to presenting our curriculum, we received feedback and on-the-ground stories from participating educators at both events.

We plan to conduct these outreach events regularly to continue to disseminate our materials and receive feedback from other educators. To date, the feedback that we have received about our curriculum has been very positive, because it genuinely appears to be filling a critical need.

6. ACKNOWLEDGMENTS

This work was made possible by the National Science Foundation under awards CNS-1065240 and DGE-1419319. We would like to thank the following contributors: Miranda Braselton, Megan Carey, Jaeyoung Choi, Alexis Conway, Isha Doshi, Henry Gan, Karina Goot, Blanca Gordo, Marian Harbach, Melia Henderson, Nicholas Henderson, Denise Huey, Fatima Ibrahim-Biangoro, Julie Ireton, Jeffrey Jacinto, James Jiang, Chan Kim, Justin Kim, Markus Krause,

Florin Langer, Jessica Larson, Itzel Martinez, Bryan Morgan, Regina Ongowarsito, Jeremy Orr, Marissa Pitta, Tim Radvan, Micky Prochaska Saglio, Gerardo Sánchez, Arany Uthayakumar, Melody Valdez, and Ketrina Yim.

7. REFERENCES

[1] N. C. S. Alliance. Stay safe online: Teach online safety. https://www.staysafeonline.org/teach-online-safety/. Website, accessed 12/3/2015.

[2] O. Astrachan, T. Barnes, D. D. Garcia, J. Paul, B. Simon, and L. Snyder. CS Principles: Piloting a new course at national scale. In *Proceedings of the 42nd ACM Technical Symposium on Computer Science Education (SIGCSE '11)*, pages 397–398, New York, NY, USA, 2011. ACM.

[3] R. Bybee, J. A. Taylor, A. Gardner, P. Van Scotter, J. Carlson, A. Westbrook, and N. Landes. The BSCS 5E instructional model: Origins and effectiveness. Technical report, Biological Sciences Curriculum Study, Colorado Springs, CO, 2006.

[4] J. T. Cacioppo, R. E. Petty, and C. Feng Kao. The efficient assessment of need for cognition. *Journal of personality assessment*, 48(3):306–307, 1984.

[5] Center on Law and Information Policy at Fordham Law School. Fordham CLIP volunteer privacy educators program. http://law.fordham.edu/assets/CLIP/2013_CLIP_VPE_Complete.pdf, 2013.

[6] Common Sense Media. K–12 digital citizenship curriculum. https://www.commonsensemedia.org/educators/curriculum. Accessed 12/1/2015.

[7] S. Egelman and E. Peer. Predicting privacy and security attitudes. *SIGCAS Comput. Soc.*, 45(1):22–28, Feb. 2015.

[8] N. C. for Missing & Exploited Children. Netsmartz workshop: Teaching materials. http://www.netsmartz.org/Resources. Website, accessed 12/3/2015.

[9] D. D. Garcia. The beauty and joy of computing (cs principles), parts 1–4. https://www.edx.org/course/beauty-joy-computing-cs-principles-part-uc-berkeleyx-bjc-1x#.VJFqqCdGzDw. edX.

[10] D. D. Garcia, B. Harvey, and L. Segars. CS Principles pilot at University of California, Berkeley. *ACM Inroads*, 3(2):58–60, June 2012.

[11] A. Lenhart, M. Madden, S. Cortesi, U. Gasser, and A. Smith. Where teens seek online privacy advice. Technical report, Pew Research Internet Project, 2013. http://www.pewinternet.org/2013/08/15/where-teens-seek-online-privacy-advice/.

[12] N. K. Malhotra, S. S. Kim, and J. Agarwal. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, December 2004.

[13] Markkula Center for Applied Ethics, Santa Clara University. Your privacy online. http://www.scu.edu/ethics-center/privacy/.

[14] MediaSmarts, 2013. http://mediasmarts.ca/.

[15] National Security Agency. NSA's Cyber Camps Make Summer School Fun. https://www.nsa.gov/public_info/press_room/2015/gencyber_summer_camps.shtml, May 2015.

[16] T. J. T. F. on Computing Curricula (Association for Computing Machinery and I.-C. Society). Computer science curricula 2013. In preparation.

[17] N. Parlante. CS101. https://class.stanford.edu/courses/Engineering/CS101/Summer2014/about. Stanford Online.

[18] A. Pentland. Big data and social physics. https://www.edx.org/course/big-data-social-physics-mitx-mas-s69x#.VJFqWSdGzDw. edX.

[19] TeachToday, 2015. http://www.teachtoday.eu/.

[20] S. B. Wicker. Wiretaps to big data: Privacy and surveillance in the age of interconnection. https://www.edx.org/course/wiretaps-big-data-privacy-surveillance-cornellx-engri1280x#.VJFpwCdGzDw. edX.

APPENDIX

A. PRIVACY PREFERENCES SCALE

1. **Online Fraud**
   - I'm concerned that if I use my credit card to buy something on the internet my card could be mischarged.
   - I'm concerned that if I use my credit card to buy something on the internet my credit card number could be obtained/intercepted by someone else.
   - I'm concerned about online organizations not being who they claim they are.
   - I'm concerned about people online not being who they say they are.
   - I'm concerned that an email containing a seemingly legitimate internet address may be fraudulent.
   - I'm concerned about online identity theft.
2. **Online Disclosure to Companies**
   - When online companies ask me for personal information, I sometimes think twice before providing it.
   - It bothers me to give personal information to so many online companies.
   - It usually bothers me when online companies ask me for personal information.
3. **Transparency and Control**
   - Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
   - A good consumer online privacy policy should have a clear and conspicuous disclosure.
   - Companies seeking information online should disclose the way the data are collected, processed, and used.
   - I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
4. **Dissemination by Others**
   - I'm concerned that an email I send someone may be printed out in a place where others could see it.
   - I'm concerned that an email I send may be read by someone else besides the person I sent it to.
   - I'm concerned that an email I send someone may be inappropriately forwarded to others.