The Teaching Privacy Curriculum

Serge Egelman[1], Gerald Friedland[1], Julia Bernd[1], Dan Garcia[2], and Blanca Gordo[1]

[1]International Computer Science Institute, Berkeley, CA,
{egelman,fractor,jbernd,blanca}@icsi.berkeley.edu
[2]University of California, Berkeley, CA
{ddgarcia}@cs.berkeley.edu

1. INTRODUCTION

Current computer science curricula aimed at high school and undergraduate students (e.g., the ACM's CS2013 [6] and the AP CS:Principles [1]) acknowledge the importance of privacy education, but do not provide content or specific lesson plans. During outreach efforts related to 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 [5]. 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 protect their personal information online. The *Teaching Privacy Project* is a privacy education curriculum centered around ten principles and offers students descriptions of how they may be putting themselves at risk online, interactive demonstrations that illustrate the concepts, and guidance on what they can do to protect themselves.

Elements of our curriculum are integrated into UC Berkeley's *Beauty and Joy of Computing* (BJC) course, which is an introductory computer science course for non-majors. The course also holds the distinction of being one of a handful of university pilots for the AP CS:Principles curriculum. The AP CS:Principles exams will be launched in 2017, but the materials have already reached many high school teachers as part of professional development programs, through the AP system and through BJC's several other outreach programs for teachers. In addition, BJC is currently working with edX to develop a Massive Open Online Course (MOOC), called BJCx, which is anticipated to reach many high school teachers as well as the college students taking it for credit.

The integration of the TPP curriculum into BJC 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 broader impact on teachers, we recently began developing the Teachers' Resources for Online Privacy Education (TROPE). In the TROPE project, we are building an online teachers' kit consisting of classroom-ready teaching modules that high school teachers and college professors can use to teach young people about *why* and *how* to protect their privacy online. TROPE also features a teachers' guide with background information and guidance on how to employ the modules in the classroom. Our goal is to empower 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.

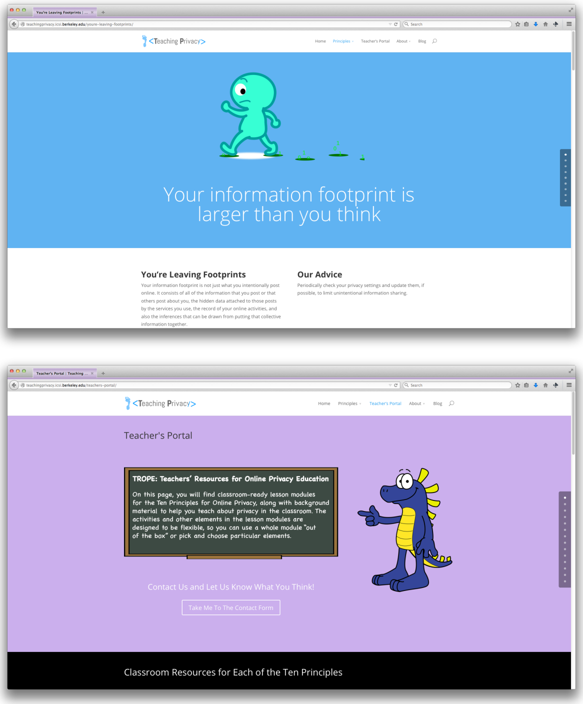
2. THE CURRICULUM

The *Teaching Privacy Project* (TPP) curriculum offers actionable guidance to general audiences on how to manage online privacy. Rather than taking a prescriptive approach (i.e., "abstinence-only") and dictating what services should and should not be used, the goal of TPP is to inform people of the risks and benefits of various online activities so that they can make informed choices. 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 and why it is important, as well as guidance for what should be done about it. The principles are as follows:

1. You're Leaving Footprints
2. There's No Anonymity
3. Information Is Valuable
4. Someone Could Listen
5. Sharing Releases Control
6. Search Is Improving
7. Online Is Real
8. Identity Isn't Guaranteed
9. You Can't Escape
10. Privacy Requires Work

Taken as a whole, the principles demonstrate the general types of threats to privacy, how they occur, why organizations engage in them, what the possible consequences are, and what people can do about it. The Teaching Privacy website, `http://www.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; and links to related resources. The principles are accompanied by 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 geolocation metadata.

We are using this youth-oriented content as the basis for developing a teachers' kit with classroom-ready learning modules and a teachers' guide. This effort, the Teachers' Resources for Online Privacy Education (TROPE), aims to


You're Leaving Footprints | ...
teachingprivacy.icsi.berkeley.edu/youre-leaving-footprints/
Search
<Teaching Privacy>
Home
Principles
Teacher's Portal
About
Blog
1
0
Teacher's Portal | Teaching ...
teachingprivacy.icsi.berkeley.edu/teachers-portal/
Take Me To The Contact Form

Your information footprint is larger than you think

You're Leaving Footprints

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.

Our Advice

Periodically check your privacy settings and update them, if possible, to limit unintentional information sharing.

Teacher's Portal

TROPE: Teachers' Resources for Online Privacy Education

On this page, you will find classroom-ready lesson modules for the Ten Principles for Online Privacy, along with background material to help you teach about privacy in the classroom. The activities and other elements in the lesson modules are designed to be flexible, so you can use a whole module "out of the box" or pick and choose particular elements.

Contact Us and Let Us Know What You Think!

Classroom Resources for Each of the Ten Principles

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

provide high school and college instructors 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 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, discussion questions, and interactive demonstrations. Each module is structured around the 5E constructivist learning model for lesson planning [2]: engagement, exploration, explanation, elaboration, and evaluation.

We are also developing a teachers' guide that provides background information and context on privacy fundamentals, classroom discussion guides and support for implementing our lesson modules, and suggested lesson plans.

All of the TROPE materials are being made available via a Teachers' Portal on `teachingprivacy.org`, where we are also implementing a discussion forum to solicit teacher feedback and answer questions.

3. DISSEMINATION AND EVALUATION

The content base and interactive learning tools on the Teaching Privacy website have generated significant interest and enthusiasm among those who have explored it. The initial TROPE materials are currently being piloted and evaluated through UC Berkeley's *Beauty and Joy of Computing* (BJC) course for non-CS majors (CS10); Gerald Friedland is currently teaching BJC, and both he and Dan Garcia are on the regular teaching rota.[1] BJC aims to increase the engagement of non-computer-science majors with technological concepts. BJC is one of only a handful of university pilots for the Advanced Placement *CS:Principles* class [4, 1], 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. We have also hosted several events, including a very popular interactive lab at UC Berkeley's open house.

In addition, we have been working closely with the *Berkeley Foundation for Opportunities in Information Technology (BFOIT)*,[2] which is based at the International Computer Science Institute (ICSI). BFOIT's mission is to support historically underrepresented ethnic minorities and women in their desire to become leaders in the fields of computer science, engineering, and information technology [3]. BFOIT organizes multi-week summer camps for minority and low-income middle school and high school students wherein they learn about computer science and information technology. Because of our close ties with BFOIT, we are able to oversee the integration of the Teaching Privacy materials into their summer programs and can directly interact with students and area high school teachers in order to evaluate the curriculum and our teaching materials.

Finally, based on the TROPE curriculum, we conducted a privacy education workshop at the 2015 ACM SIGCSE conference. In addition to presenting our curriculum, we received feedback and on-the-ground stories from participating educators. We hope to conduct this workshop annually in order to continuously update and improve our materials.

4. ACKNOWLEDGMENTS

This work was made possible by the National Science Foundation under award DGE-1419319.

5. REFERENCES

[1] 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.

[2] 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.

[3] O. S. L. Crutchfield, C. D. Harrison, G. Haas, D. D. Garcia, S. M. Humphreys, C. M. Lewis, and P. Khooshabeh. Berkeley Foundation for Opportunities in Information Technology: A decade of broadening participation. *Trans. Comput. Educ.*, 11(3), Oct. 2011.

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

[5] 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/`.

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

[1] `http://bjc.berkeley.edu`

[2] `http://www.bfoit.org`