Last Updated: October 10, 2014

Digital Trust Foundation

Privacy Education for Youth

Request for Proposals

Proposal Deadline: November 21, 2014, by 11:59 PM PT

Program Goals

1. To increase the privacy resilience of children and teens in the face of complex data sharing environments.

2. To help children and teens develop skills and resources to protect them in the digital environment throughout life.

Summary

The Beacon settlement agreement directed the Digital Trust Foundation to invest in educating Internet users on how to protect themselves and their information from online threats.[1] The Foundation intends to invest $1,000,000 to fund privacy education projects focused on young people residing in the United States. We anticipate entertaining proposals for projects of various sizes, with budgets in the range of $50,000 and $200,000. Exceptional projects with budgets outside this range may be considered.

Why Invest in Privacy Education for Youth?

Educators, advocates, policymakers, and the public recognize the importance of technology and the Internet to our economy and society. Over the last three decades, there has been increasing emphasis on teaching youth and adults alike the skills that they need to use technology in their education, work, and social lives. The skills needed to successfully and safely navigate technology and the Internet include everything from the technical skills of operating a computer to the cognitive skills that allow a user to interpret information and communicate. These skills are currently described as digital literacy.

---

[1] See the agreement for more details about the case.

The concept of digital literacy is evolving in the research literature and in policymaking circles in the United States. While there is widespread agreement that people of all ages need support in accessing and using the Internet for a variety of life functions, there is less agreement about how and where to teach these skills. Children and teens are prime candidates for digital literacy education because they are growing up in a digital environment that they will use for the rest of their lives. The federal government has not issued standards for digital literacy curricula for the K-12 realm; states, school districts, and non-governmental organizations are experimenting with various curricula and standards.[2]

One component of digital literacy is understanding how and when to protect oneself and personal information online. Protecting privacy involves understanding how data are collected and used online, the controls available around such collection and use, the availability of privacy-enhancing technologies, and how to know whom to trust when communicating online. Young people are a target population for privacy education because sharing personal information is crucial to identity and relationship formation. Their entire lives will to some degree be documented online, the consequences of which are unknown.

Youth and young adults have strong expressed preferences for privacy, and they also appear to be using privacy settings on social networking sites.[3] A 2012 survey of youth and adults found that 81% of teenagers on social networks have adjusted their privacy settings,[4] which is a higher proportion than past studies have found. Use of privacy settings does not necessarily indicate understanding of the settings or website privacy policies,[5,6] suggesting that youth may need more education on how to protect themselves online.

---

2 Belshaw, D. (2012). What is 'digital literacy'? A Pragmatic investigation (Doctoral dissertation, Durham University). Available at: http://dmlcentral.net/sites/dmlcentral/files/resource_files/doug-belshaw-edd-thesis-final.pdf

3 Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies?. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864

4 Hart Research Associates. (2012). The Online General Gap: Contrasting attitudes and behaviors of parents and teens. The Family Online Safety Institute. Available at: http://www.fosi.org/images/stories/research/hartreport-onlinegap-final.pdf

5 Madejski, M., Johnson, M., & Bellovin, S. M. (2012). A study of privacy settings errors in an online social network. Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on (pp. 340-345). IEEE. Available at: http://maritzajohnson.com/publications/2012-sesoc.pdf

6 Marwick, A. E. & boyd d. (2014). Networked privacy: How teenagers negotiate context in social media. New Media & Society. Available at: http://nms.sagepub.com/content/early/2014/07/19/1461444814543995

According to the Crimes Against Children Research Center, current online privacy and safety curricula for youth are not evidence-based, cover a range of risks in too little time, and are misaligned with the most common online threats. Their 2011 white paper on online safety programs for youth noted that there is a lack of evaluation of these programs. All evidence of effectiveness thus far is anecdotal.[7]

An expert panel convened by the Aspen Institute and the MacArthur Foundation recently recommended that schools teach digital, media, and socio-emotional literacies as basic skills that will support youth in both online and offline environments. These literacies will allow youth to protect themselves online from an early age and thus maximize their benefit and enjoyment of the online environment. The panel recommended that these skills be required for teachers as well. It also recommended more research into best practices for teaching these literacies.[8]

A 2011 federal task force reached a similar conclusion. The Online Safety and Technology Working Group found that "civil, respectful behavior online is less conducive to risk" and called digital literacy "the cornerstone of Internet safety." It recommended that digital literacy education promote social norms of non-risky online behavior, rather than use scare tactics. A social norms approach to reducing risky behavior has been shown to be more effective than fear-based education.[9]

Protecting privacy for everyone online will require a mix of strategies, including policy, social norm change, technology development, and education. Strategies directed at youth privacy will need to recognize different levels of sophistication for youth of different ages and will need to respect different privacy norms. There is a need for effective privacy education that will give youth the skills they need to protect themselves online for their entire lives. Privacy education should not only include teaching youth to protect their data, but also helping them understand the implications of the choices available to them[10] and how choice is defined and constrained by business models and public policy. Privacy

---

7 Jones L. M. & Finkelhor D. (2011). Increasing Youth Safety and Responsible Behavior Online: Putting in Place Programs that Work. Family Online Safety Institute. Available at: http://www.fosi.org/images/stories/resources/fosi_whitepaper_increasingyouthsafety_d9.pdf

8 Task Force on Learning and the Internet. (2014). Learner at the Center of the Networked World. The Aspen Institute. Available at: http://csreports.aspeninstitute.org/Task-Force-on-Learning-and-the-Internet/2014/report

9 Online Safety and Technology Working Group. (2010). Youth Safety on a Living Internet. Available at: http://www.ntia.doc.gov/legacy/reports/2010/OSTWG_Final_Report_070610.pdf

10 Berson, I. R., & Berson, M. J. (2006). Children and Their Digital Dossiers: Lessons in Privacy Rights in the Digital Age. International Journal of Social Education, 21(1), 135-147. Available at: http://files.eric.ed.gov/fulltext/EJ782348.pdf

education, and digital literacy education more broadly, should give youth the skills they need to thrive in digital environments, even as technology and communication media change over time.

Eligible Projects

The Digital Trust Foundation invites proposals to pursue one of three strategies described below. For each strategy, we identify the minimum requirements and criteria for priority projects.

IMPORTANT: Applicants may only submit one proposal for funding under this program area.

Strategy 1.1: Implementation & Assessment of Online Privacy Education Programs

The Beacon settlement agreement directed the Foundation to invest in educating Internet users on how to protect themselves and their information from online threats. The Foundation believes that focusing on young people will yield long-term benefits. In particular, the Foundation sees a need to evaluate existing online privacy education programs to determine what messages and strategies are most effective at giving youth the skills they need to be safe, productive digital citizens for their entire lives.

The Foundation may fund multiple projects under this strategy.

Project Requirements

- We expect to fund multiple projects with diverse budgets in the range of $50,000 to $200,000. We may consider exceptional projects outside of this range.
- Must implement a privacy education program for youth who are between 4 and 18 years old (projects can focus on a sub-segment of this age group).
- Must evaluate the implementation of the program.
- Must be implemented in the United States.
- Education program must:
  - Present youth with digital literacy information or skills that can be applied to online privacy decisions.
  - Provide youth with skills that can be applied in different digital environments.
  - Help youth make decisions about how and when to share information online and the

implications of the choices available.
- We will not fund new curriculum or program development. However, funds may be used to update and implement existing curricula or programs.
- We are interested in funding projects implemented inside and outside of the school environment, including settings such as after-school programs, faith-based organizations, or community centers.
- Evaluation should incorporate recognized digital literacy core competencies or skills, such as the Socio-Emotional Learning Core Competencies[11] and/or the Essential Competencies of Digital Literacy.[12]

Priority Projects

The Foundation will entertain all proposals that meet the basic project requirements outlined above. However, the Foundation has particular interest in projects with one or more of the following characteristics. Projects with these characteristics will be prioritized in funding decisions:
- Demonstrate sustainability of the content delivery mechanism. For example, a project that trains educators to be resources on online privacy issues may be more sustainable than a project that sends college students into a school to talk about online privacy.
- Focus on youth of color, low-income youth, or English language learners.

[11] Collaborative for Academic, Social, and Emotional Learning. (nd). Social and Emotional Learning Core Competencies. Available at: http://www.casel.org/social-and-emotional-learning/core-competencies.

[12] Hobbs, R. (2010). Digital and Media Literacy: A Plan of Action. A White Paper on the Digital and Media Literacy Recommendations of the Knight Commission on the Information Needs of Communities in a Democracy. *Aspen Institute*. Available at: http://www.knightcomm.org/wp-content/uploads/2010/12/Digital_and_Media_Literacy_A_Plan_of_Action.pdf

Strategy 1.2: Online Privacy Campaigns for Youth

Looking to the success of public health media campaigns, such as the Truth Campaign for preventing youth tobacco use, the Foundation invites proposals for media campaigns to educate youth about online safety and privacy. Messages used in media campaigns must be audience tested or crafted based on media campaign best practices. When crafted well, mass media campaigns can be a cost-effective way to change specific behaviors and social norms in a relatively large population.[13] These campaigns should reinforce messages that youth may be hearing from their families, schools, and other institutions teaching online privacy.

The Foundation may fund multiple projects under this strategy.

Project Requirements

- We expect to fund multiple projects with diverse budgets in the range of $50,000 to $200,000. We will consider exceptional projects outside of this range.
- Campaign must:
  - Be targeted to youth who are between 4 and 18 years old (projects can focus on a sub-segment of this age group).
  - Substantially and primarily benefit youth residing in the United States.
  - Respond to a recognized need for online privacy education for youth.
  - Present youth with digital literacy information or skills that can be applied to online privacy decisions. Should incorporate recognized digital literacy core competencies or skills, such as the Socio-Emotional Learning Core Competencies[14] and/or the Essential Competencies of Digital Literacy.[15]
  - Be evidence based or audience tested prior to deployment.
  - Apply best practices drawn from other public awareness campaigns, such as those described on page 9 of Increasing Youth Safety and Responsible Behavior Online: Putting in Place Programs that Work.[16]

---

[13] Wakefield, M. A., Loken, B., & Hornik, R. C. (2010). Use of mass media campaigns to change health behaviour. *The Lancet*, *376*(9748), 1261-1271. Available at: http://cms.csom.umn.edu/marketinginstitute/research/documents/Useofmassmediacampaignstochangehealthbehaviour.pdf

[14] Collaborative for Academic, Social, and Emotional Learning. (nd). Social and Emotional Learning Core Competencies. Available at: http://www.casel.org/social-and-emotional-learning/core-competencies.

[15] Hobbs, R. (2010). Digital and Media Literacy: A Plan of Action. A White Paper on the Digital and Media Literacy Recommendations of the Knight Commission on the Information Needs of Communities in a Democracy. *Aspen Institute*. Available at: http://www.knightcomm.org/wp-content/uploads/2010/12/Digital_and_Media_Literacy_A_Plan_of_Action.pdf

[16] Jones LM & Finkelhor D. (2011). Increasing Youth Safety and Responsible Behavior Online: Putting in

- Campaign may be deployed in any type of media.
- Campaign may address digital literacy in all digital environments or focus on a particular environment, such as mobile environments.

Priority Projects

Priority will be given to project proposing novel dissemination strategies, such as integrating messages into television shows, movies, digital media, games, social media, or other entertainment content.

Place Programs that Work. Washington, DC: Family Online Safety Institute. Available at: http://www.unh.edu/ccrc/pdf/fosi_whitepaper_increasingyouthsafety_d9.pdf

Strategy 1.3: Online Privacy Messaging Best Practices White Paper

The Foundation invites proposals to research and write a paper that presents the current evidence base for communications strategies to effect behavior or social norm change among youth. The audience for the paper will be online privacy education program and media campaign developers. There has been little evaluation of online privacy, Internet safety, and other digital literacy education programs. Program and campaign developers must look to other fields, such as public health, to identify communication strategies and messages that are effective at changing behavior.[17] There is a need for a practical review of this literature that is written for developers working on online privacy initiatives. The goal is to make it easier for these developers to integrate evidence-based messages into their work.

The Foundation will fund one grant.

Project Requirements

- Project budget must be $50,000 or less.
- White paper must present communication and messaging strategy best practices based on published literature. Best practices may be drawn from diverse fields of study.
- When possible, best practices should be specific to presenting information to youth.
- Literature and best practices should be presented for a practitioner audience. It must be presented in a way that could be easily applied to online privacy education programs and campaign development and implementation.
- Researcher or team should have experience with behavior change, public education campaign, or messaging research.
- Researcher or team must show a track record of translating research for practical applications.
- Project plan and budget should include time for peer review of later draft of paper.

[17] Jones L.M. (2010). The Future of Internet Safety Education: Critical Lessons from Four Decades of Youth Drug Abuse Prevention. Berkman Center for Internet and Society. Available at: http://publius.cc/future_internet_safety_education_critical_lessons_four_decades_youth_drug_abuse_prevention

Eligible Applicants for All Strategies

- Non-profit organizations
- For-profit corporations
- Universities or other academic institutions
- Government entities, including schools or school districts
- Qualified individuals are only eligible for Strategy 1.3.

Applications may be submitted by domestic and international entities. Applicants must demonstrate that the proposed project substantially and primarily benefits people residing in the United States.

Evaluation Requirements

The Foundation believes that well-crafted program evaluation can strengthen organizations and improve future work in this field. We seek to contribute to the growing body of evidence related to digital privacy. At the same time, we do not want to burden grantees with unnecessary or onerous reporting requirements.

Therefore, we will ask grantees to participate in a set of straightforward evaluation activities. The Foundation will provide grantees with simple reporting forms to gather evaluation information, including outputs, successes, challenges, and lessons learned. Grantees should also be prepared to participate in Foundation-level evaluation activities that may take place throughout the term of the grant (such as surveys and interviews conducted by the Foundation). Applicants should plan to have a staff person assigned to meet the reporting and Foundation-level evaluation requirements.

In addition, all proposals under Strategy 1.1 (Implementation & Assessment of Online Privacy Education Programs), as well as proposals for grants of over $200,000 for Strategy 1.2 (Online Privacy Campaigns for Youth) are required to submit a formal evaluation plan for monitoring their progress, as described below.

Strategy 1.1 (Implementation & Assessment of Online Privacy Education Programs) Evaluation Requirement

One of the goals of Strategy 1.1 is to contribute to the evidence base of what works in online privacy education for youth. Therefore, a formal evaluation plan is required for all Strategy 1.1 proposals. The plan should include a description of the evaluation questions,

indicators that will be tracked, plans for data collection, and who will be responsible for carrying out the evaluation.

Strategy 1.2 (Online Privacy Campaigns for Youth) Evaluation Requirement

For Budgets Less Than $200,000:

While a formal evaluation plan is not required, grantees will still be expected to track basic information on project implementation and results using forms provided by the Foundation. We may also ask grantees to participate in Foundation-level evaluation.

For Budgets Greater Than $200,000:

A formal evaluation plan is required for all Strategy 1.2 proposals over $200,000. The plan should include a description of the evaluation questions, indicators that will be tracked, plans for data collection, and who will be responsible for carrying out the evaluation. The evaluation budget should represent no more than 15 percent of the total project budget.

Strategy 1.3 (Online Privacy Messaging Best Practices White Paper) Evaluation Requirement

A formal evaluation plan is not required. However, grantees will still be expected to track basic information on project implementation and results. We may also ask grantees to participate in Foundation-level evaluation.

Application Process & Timeline

For a list of materials to submit, see the application packet and checklist provided on the Foundation website.

November 21, 2014: Full proposals due.

Late November/Early December 2014: The program officer may send follow-up questions to some applicants about proposals, budgets, or organization finances.

February 2015: The Foundation communicates funding decisions to applicants.

Mid-February 2015: The Foundation and grantees enter into contract.

About the Digital Trust Foundation

In 2007, a class action lawsuit was filed in the United States District Court of the Northern District of California against Facebook on behalf of 3.6 million users of Facebook concerning its "Beacon" program. KamberLaw represented the plaintiffs in this action and Cooley LLP represented Facebook. This suit was settled in 2009 and was granted final approval by the Hon. Richard Seeborg in March 2010. As part of the settlement, the parties created the Foundation (the Digital Trust Foundation) "the purpose of which shall be to fund projects and initiatives that promote the cause of online privacy, safety, and security." The case settled for $9.5 million, with the Foundation receiving approximately $6.7 million after attorney's fees, payments to plaintiffs, and administrative costs. There were four objectors to the settlement, two of whom appealed the approval to the Ninth Circuit Court of Appeals and subsequently the Supreme Court. But ultimately, in November 2013, the appeals were rejected and the Foundation was funded. The Foundation will distribute more than $6 million and will close its doors once all of the grants have been distributed and completed.

To learn more about the Digital Trust Foundation, visit our website.