Last Updated: March 27, 2015

Digital Trust Foundation

Assessing, Preventing, and Addressing Digital Abuse

Request for Proposals

***Proposal Deadline*: May 7, 2015, by 11:59 PM PT**

Program Goals

1. To document the prevalence and severity of various forms of digital abuse.

2. To understand and support digital abuse prevention strategies.

3. To contribute constructively to the digital abuse policy debate.

4. To provide resources to organizations that support digital abuse victims.

Summary

The Digital Trust Foundation has found several gaps in digital abuse research and action. To address these gaps, the Foundation intends to fund (1) empirical research to understand the prevalence of various forms of digital abuse; (2) implementation and evaluation of digital abuse prevention strategies; and (3) organizations that provide direct services to victims and projects that contribute to the digital abuse policy debate. 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 of this range may be considered.

Background and Definitions

Online harassment and abuse have existed since the early days of the Internet. Seventy-three percent of adults report having witnessed online harassment, and 40 percent report having experienced it themselves.[1] There are many

[1] Pew Research Center. (2014). Online Harassment. Available at: http://www.pewinternet.org/2014/10/22/online-harassment/.

overlapping terms for various forms of online harassment and abuse, making these experiences difficult to discuss and study precisely. In this RFP, we will focus on three behaviors found in the literature: cyberstalking, cyberbullying, and digital domestic violence, as defined below. We intend to give priority to proposals that address these forms of abuse; however, we will entertain proposals focused on any form of digital abuse, not just those discussed in the RFP.

Cyberstalking

Stalking is defined as "repeated harassing and threatening behavior."[2] Sixteen percent of women and four percent of men in the United States report having been stalked at some point in their lives.[3] Two to three percent of adults in the United States – or approximately 5.9 million people – report having been stalked or harassed some time in the last 12 months. By comparison, 5.2 million violent crimes were reported in the same time period.[4] People under the age of 25, Native Americans, multi-racial people, and low-income people are the most likely to be stalking victims.[5]

Although many reports distinguish between cyberstalking and offline stalking, prevalence studies show that stalking victims may experience a combination of online and offline stalking.[6,7] Estimates of cyberstalking vary, in part due to different ways of categorizing online forms of stalking; one study estimates that approximately 25 percent of stalking victims experience cyberstalking.[8] Eighty

---

[2] Lipton J.D. (2011). Combating cyber-victimization. *Berkeley Tech. LJ*, 26, 1103. Available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1901&context=btlj.

[3] Black M.C., Basile K.C., Breiding M.J., et al. (2011). The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report. National Center for Injury Prevention and Control, Centers for Disease Control and Prevention. Available at: http://www.cdc.gov/violenceprevention/pdf/nisvs_report2010-a.pdf

[4] Baum K., Catalano S., Rand M., et al. (2009). Stalking Victimization in the United States. U.S. Department of Justice. Available at: https://www.victimsofcrime.org/docs/src/baum-k-catalano-s-rand-m-rose-k-2009.pdf?sfvrsn=0.

[5] Ibid.

[6] Black M.C., Basile K.C., Breiding M.J., et al. (2011). The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report. National Center for Injury Prevention and Control, Centers for Disease Control and Prevention. Available at: http://www.cdc.gov/violenceprevention/pdf/nisvs_report2010-a.pdf

[7] Baum K., Catalano S., Rand M., et al. (2009). Stalking Victimization in the United States. U.S. Department of Justice. Available at: https://www.victimsofcrime.org/docs/src/baum-k-catalano-s-rand-m-rose-k-2009.pdf?sfvrsn=0.

[8] Ibid.

percent of victims reported receiving unwanted phone calls, voice mails, and/or text messages.[9]

Cyberbullying

Cyberbullying can be used to describe a range of "tormenting, threatening, harassing, humiliating, embarrassing, or otherwise targeting" behaviors.[10] In the media, cyberbullying is often discussed in the context of youth,[11] but anyone can be a victim or perpetrator of cyberbullying. In fact, 18 percent of adult Internet users in the United States report experiencing some form of serious harassment online.[12] Cyberbullying often begins with a single perpetrator targeting a victim and then evolves into so-called mobbing behavior with a group of perpetrators targeting the victim.[13] Young women are more likely than young men and older women to experience severe forms of harassment: stalking and sexual harassment. African American and Latino Internet users are more likely than white users to experience online harassment.[14] Some legal scholars contend that the targeting of women and people of color on the Internet discourages their online participation and that cyberbullying should be treated as civil rights violations from a legal standpoint.[15]

Cyberbullying among youth has received more attention than other forms of online harassment and abuse because of high-profile incidents involving

---

[9] Black MC, Basile KC, Breiding MJ, et al. (2011). The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report. National Center for Injury Prevention and Control, Centers for Disease Control and Prevention. Available at: http://www.cdc.gov/violenceprevention/pdf/nisvs_report2010-a.pdf

[10] Lipton, JD. (2011). Combating cyber-victimization. *Berkeley Tech. LJ*, *26*, 1103. Available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1901&context=btlj.

[11] See, e.g., Sengupta S. (2013). Warily, Schools Watch Students on the Internet. New York Times. Available at: http://www.nytimes.com/2013/10/29/technology/some-schools-extend-surveillance-of-students-beyond-campus.html.

[12] Pew Research Center. (2014). Online Harassment. Available at: http://www.pewinternet.org/2014/10/22/online-harassment/.

[13] Lipton, JD. (2011). Combating cyber-victimization. *Berkeley Tech. LJ*, *26*, 1103. Available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1901&context=btlj.

[14] Pew Research Center. (2014). Online Harassment. Available at: http://www.pewinternet.org/2014/10/22/online-harassment/

[15] Citron DK. (2009). Cyber civil rights. *Boston University Law Review*, *89*, 61-125. Available at: https://www.bu.edu/law/central/jd/organizations/journals/bulr/volume89n1/documents/CITRON.pdf.

youth.[16] Prevalence rates of cyberbullying victimization and perpetration vary widely due to a lack of standard definition and measurement tools. Victimization rates are estimated to be four percent to 72 percent (across a range of age groups), and perpetration rates range from three percent to 36 percent.[17,18] The Cyberbullying Research Center estimates that approximately 24 percent of middle and high school students have been cyberbullied.[19] Prevalence based on various characteristics, including age, gender, disability, and sexual orientation, are even less well known due to conflicting research findings and limited examination.[20] Cyberbullying among youth is more likely to occur online than via phone or text message.[21] Cyberbullying among youth is generally part of a larger pattern of bullying happening offline.[22]

Digital Domestic Violence

Domestic violence and sexual harassment are also increasingly taking online forms. One form, known as cyberexploitation, occurs when sexually graphic images of a person are distributed without his/her consent (this form is sometimes referred to as revenge porn). The images may have been shared with a partner who then betrays the victim's trust and shares them more widely,

---

[16] Tokunaga RS. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, 26(3), 277-287. Available at: http://icbtt.arizona.edu/sites/default/files/tokunaga,_r_cyberbullying.pdf.

[17] Kowalski RM, Giumetti GW, Schroeder AN, et al. (2014). Bullying in the Digital Age: A Critical Review and Meta-Analysis of Cyberbullying Research Among Youth. *Psychological Bulletin*, 140(4): 1137. Available at: http://www.homeworkmarket.com/sites/default/files/q2/07/03/cyberbulling_metaanalysis.pdf.

[18] Nixon CL. (2014). Current perspectives: the impact of cyberbullying on adolescent health. Adolescent Health, Medicine, and Therapeutics, 5:143. Available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4126576/.

[19] Connect Safely. (2014). A Parents' Guide to Cyberbullying. Available at: http://www.connectsafely.org/wp-content/uploads/cyberbullying_guide.pdf.

[20] Levy NL, Cortesi S, Gasser U, et al. (2012). Bullying in a Networked Era: A Literature Review. The Berkman Center for Internet and Society at Harvard University: Kinder & Braver World Project. Available at: http://dmlcentral.net/sites/dmlcentral/files/resource_files/ssrn-id2146877.pdf.

[21] Ybarra M, boyd d, Korchmaros J, et al. (2012). Defining and measuring cyberbullying within the larger context of bullying victimization. *Journal of Adolescent Health*, 51(1): 53. Available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3383604/.

[22] Notar CE, Padgett S, Roden J. (2013). Cyberbullying: A Review of the Literature. *Universal Journal of Educational Research*, 1(1): 1. Available at: http://www.hrpub.org/download/201306/ujer.2013.010101.pdf.

or the images may have been obtained through secret recording or hacking into files.[23] Revenge porn victims may experience serious consequences, including anxiety, depression and loss of job and educational opportunities.[24] It is unclear how prevalent revenge porn is, as little published empirical research exists.

Why Invest in Assessing, Preventing, and Addressing Online Abuse?

Some legal scholars contend that state and federal laws meant to address offline stalking, bullying, and other harassment are not sufficient to deal with analogous crimes committed online. For example, harassment and stalking laws often require physical proximity between the victim and perpetrator. Victims may not know who the perpetrator is or where they are located, and this anonymity can make their harassment more menacing. Many laws also require a credible threat directed at the victim, not recognizing that continued online harassment and shaming exacts a substantial emotional toll on the victim. [25]

The Digital Trust Foundation has found several gaps in digital abuse research and action. First, there is a need for more prevalence and trend data on all forms of digital abuse. For example, there is a need for data on the prevalence of cyberexploitation (including so-called revenge porn and sextortion). More data are needed on demographics of people who experience cyberbullying. For types of digital abuse that have been better studied, such as youth cyberbullying, there is still a need for data on the experiences of sub-populations, such as children with disabilities, elementary school-aged children, and LGBTQ youth.

Second, there is a need for more exploration of what works and what doesn't work for prevention of all forms of digital abuse. For example, cyberbullying

---

[23] Franks MA. (2014). Combating Non-Consensual Pornography: A Working Paper. Available at: http://www.endrevengeporn.org/main_2013/wp-content/uploads/2013/10/Franks-NCP-Working-Paper-9.18.pdf.

[24] Citron DK & Franks MA. (2014). Criminalizing Revenge Porn. *Wake Forest Law Review*, 49: 345. Available at: http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2424&context=fac_pubs.

[25] Lipton J.D. (2011). Combating cyber-victimization. *Berkeley Tech. LJ*, 26, 1103. Available at: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1901&context=btlj.

counter-measures that are often recommended to schools, such as technology restrictions and zero tolerance policies, have been found to be ineffective and possibly harmful. [26]

Finally, more resources and support systems are needed for victims of digital abuse. For example, local law enforcement officials need training on how to respond to and document reports of digital abuse. Legislatures need research and analysis about the limitations of existing laws to handle digital abuse.

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.

Strategy 3.1: Understanding Digital Abuse Prevalence

The Digital Trust Foundation will fund empirical research to understand the prevalence of various forms of digital abuse.

The Foundation may fund multiple projects under this strategy. **We will consider only one proposal per principal investigator for this strategy.**

Project Requirements

- We expect to fund multiple projects with diverse budgets of up to $200,000. Exceptional projects outside this range may be considered.
- Research can examine the prevalence of any form of digital abuse, including stalking, harassment, cyberexploitation, or cyberbullying.
- Projects may examine victim and/or perpetrator prevalence.

[26] Levy NL, Cortesi S, Gasser U, et al. (2012). Bullying in a Networked Era: A Literature Review. The Berkman Center for Internet and Society at Harvard University: Kinder & Braver World Project. Available at: http://dmlcentral.net/sites/dmlcentral/files/resource_files/ssrn-id2146877.pdf.

- Projects must:
    - Include a quantitative component. We will consider projects that include a qualitative component that documents victims' and/or perpetrators' experiences.
    - Include an online dissemination component that shares results with the advocacy community and/or general public.
    - Substantially and primarily benefit people residing in the United States.
- The indirect rate for universities is capped at 10% of the total project budget. Other non-profits may include a reasonable overhead rate in the project budget.

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 may be prioritized in funding decisions:

- Projects that examine prevalence for cyberbullying, cyberstalking, or digital domestic violence.
- Projects that fill a research gap. Proposals must demonstrate how the project will fill a research gap.
- Projects that compare digital abuse prevalence across age groups, including both youth and adults.

Strategy 3.2: Understanding Digital Abuse Prevention

The Digital Trust Foundation will fund implementation and evaluation of digital abuse prevention strategies.

The Foundation may fund multiple projects under this strategy. **We will consider only one proposal from each organization under this strategy.**

Project Requirements

- We expect to fund multiple projects with diverse budgets up to $100,000. Exceptional projects outside this range may be considered.
- Projects must implement and evaluate an evidence-based digital abuse prevention program. Projects may be a pilot program, may involve scaling a pilot program for a wider audience, or may be continued implementation of an existing prevention program.
- Projects can test new prevention strategies, but proposals must include a theory of change or evidence base to support the proposed strategies.
- Projects can address any form of digital abuse, including stalking, harassment, cyberexploitation, or cyberbullying.
- Proposed projects must include a method and plan for evaluating the effectiveness of the prevention strategy. Evaluation may represent up to 15 percent of the project budget. See Evaluation Requirements on page 11.
- Projects must substantially and primarily benefit people residing in the United States.
- We cannot fund litigation or lobbying.

Priority Projects

The Foundation will entertain all proposals that meet the basic project requirements outlined above. However, the Foundation has particular interest in projects that address cyberbullying, cyberstalking, or digital domestic violence.

Strategy 3.3: Supporting Digital Abuse Victims

The Digital Trust Foundation will fund organizations that provide direct services to victims and projects that contribute to the digital abuse policy debate.

The Foundation may fund multiple projects under this strategy. **We will consider only one proposal from each organization under this strategy.**

Project Requirements

- We expect to fund multiple projects with diverse budgets up to $100,000. Exceptional projects outside this range may be considered.
- Examples of eligible projects include:
  - Providing information and/or support to digital abuse victims. We cannot fund legal representation.
  - Providing digital abuse training or educational materials to criminal justice stakeholders, such as local law enforcement, attorneys, or judges.
  - Conducting research and analysis on policy and legal solutions for digital abuse.
  - Making available digital abuse legal and policy research and analysis to interested advocates and legislative bodies.
- Projects with budgets greater than or equal to $200,000 must include a formal program evaluation. See Evaluation Requirements on page 11.
- Projects must substantially and primarily benefit people residing in the United States.
- We cannot fund litigation or lobbying.

Priority Projects

The Foundation will entertain all proposals that meet the basic project requirements outlined above. However, the Foundation has particular interest in projects that address cyberbullying, cyberstalking, or digital domestic violence.

Eligible Applicants for All Strategies

- Non-profit organizations
- Universities or other academic institutions
- Government entities
- For-profit companies
- Qualified individuals are only eligible for Strategy 3.1.

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 online privacy, safety, and security. At the same time, we do not want to burden grantees with unnecessary or onerous reporting requirements.

Therefore, we will ask all 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 or its evaluators). Applicants should plan to have a staff person assigned to meet the reporting and Foundation-level evaluation requirements.

Aside from the requirements described above, Strategy 3.1 projects are not required to have an evaluation component, regardless of budget size. All Strategy 3.2 projects are required to have an evaluation component. Strategy 3.3 projects with budgets equal to or greater than $200,000 are required to have an evaluation component.

<u>Strategy 3.2 Projects</u>

A formal evaluation plan is required for all Strategy 3.2 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. We strongly recommend that this plan be developed by a staff member or consultant with formal program evaluation experience or training. The evaluation budget should represent no more than 15 percent of the total project budget.

Strategy 3.3 Projects with Budgets Equal to or Greater Than $200,000

A formal evaluation plan is required for Strategy 3.3 proposals with budgets equal to or greater than $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. We strongly recommend that this plan be developed by a staff member or consultant with formal program evaluation experience or training. The evaluation budget should represent no more than 15 percent of the total project budget.

Application Process & Timeline

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

May 7, 2015: Full proposals due.

Late May 2015: The program officer may send follow-up questions to some applicants about proposals, budgets, or organization finances.

Early July 2015: The Foundation communicates funding decisions to applicants.

July 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.