Digital Trust Foundation

Final Report

January 23, 2019

Prepared by
Samantha Graff and Christine Fry

Executive Summary

This report summarizes the operations and grantmaking of the Digital Trust Foundation, established in a litigation settlement with Facebook to make grants involving education, digital privacy, and online safety. The purpose of this report is to provide a transparent accounting of how the Foundation was managed and how the money was spent, not an independent analysis of the Foundation's outcomes. The authors of this report were consultants to Digital Trust through most of its existence.

The Digital Trust Foundation received $6.7 million in *cy pres* funds in January 2014 as a result of the settlement in *Lane v. Facebook*, known as the Facebook Beacon case. From 2014 to 2018, the Foundation spent down this corpus, disbursing just under $6.5 million as grants with an estimated administrative overhead of less than 6 percent. No director received any compensation. The Foundation perhaps underspent on administrative processes, as the grant tracking would have benefited from more staff oversight.

The Foundation focused on four areas: privacy education for youth, research on socioeconomic status and privacy, the problem of digital abuse, and general funding for online privacy, safety, and security. These efforts led to the development of new, freely available curricula for students, many research papers on privacy, empirical research on the problem of digital abuse including greater attention to "sextortion," and better-informed government and private sector policy and practice. (See Appendix for a summary of grant outputs.) The Foundation played a major role in launching academic efforts on SES and privacy, a topic rarely discussed in the literature prior to Digital Trust's investment of $1.5 million in the field.

Several class members and advocates opposed the Digital Trust Foundation's formation, which also received judicial criticism although it was ultimately upheld. The critiques focused on the potential for biased, ineffective grantmaking. But Digital Trust demonstrated that *cy pres* funds can be responsibly and effectively disbursed by an expert-led foundation. Digital Trust practiced a culture of accountability by implementing a strategic, consensus-based grantmaking process; adopting a conflicts of interest policy; issuing open RFPs; monitoring grants; and releasing this report for public consumption. Compared to standard *cy pres*, which often results in unsupervised, open-ended gifts to litigants' favored institutions, the Foundation supported diverse organizations with specific agendas in the promotion of education, digital privacy, and online safety.

Digital Trust Foundation Final Report

This report summarizes the operations and grantmaking of the Digital Trust Foundation, established in a litigation settlement with Facebook to make grants involving education, digital privacy, and online safety. The purpose of this report is to provide a transparent accounting of how the Foundation was managed and how the money was spent, not an independent analysis of the Foundation's outcomes. The authors of this report were consultants to Digital Trust through most of its existence. Parts I and II aim to provide an objective summary of the Foundation's operations and grantmaking, while Part III offers some analysis and reflections from the authors' point of view.

I. OPERATIONS, FROM SETUP TO WINDDOWN

The Beacon Lawsuit: 2007 – 2013

In 2007, nineteen plaintiffs filed *Lane v. Facebook*, a class action lawsuit on behalf of 3.6 million users of Facebook concerning its Beacon program. The Beacon program updated a user's Facebook profile to announce certain actions that the user had taken—in Lane's case, purchasing a ring for his wife—on the websites of third parties who had contracted with Facebook to participate in the program. Since the Beacon program did not require users' consent, many complained that Beacon was violating their privacy by broadcasting personal information to their Facebook "friends" without prior notice or approval.

Scott Kamber of KamberLaw represented the plaintiffs in *Lane v. Facebook*, and Michael Rhodes of Cooley LLP represented Facebook. In March 2010, the U.S. District Court approved a settlement under which Facebook agreed to terminate the Beacon program permanently and pay a total of $9.5 million.[1] The settlement included a *cy pres* distribution, which is a common remedy in class actions whereby, instead of direct payments, class members receive an indirect benefit (usually through defendant donations to one or more mutually agreed-upon nonprofits doing work related to the issue in the case). The *cy pres* doctrine is a solution to the problem of class action funds that are infeasible to distribute in instances like this where each individual class member's award would be de minimus.

Although a *cy pres* remedy in a case like this is not atypical, the *Lane v. Facebook* settlement was unusual in that it established a charity, the Digital Trust Foundation, to distribute the approximately $6.7 million settlement funds that remained after attorneys' fees, administrative costs, and payments to class representatives. As set forth in its bylaws, the Foundation's mission is to "fund and sponsor programs designed to educate users, regulators and enterprises regarding critical issues relating to protection of identity and personal information online through user control, and the protection of users from online threats." The idea behind

[1] Lane v. Facebook, Inc., 2010 U.S. Dist. LEXIS 24762, 2010 WL 9013059.

establishing a new grantmaking organization was that the lawyers for both parties were not comfortable selecting in real-time particular nonprofit recipients of the settlement funds.[2]

The Foundation's Articles of Incorporation provide for a three-member unpaid board. Initially, one was selected by plaintiffs' counsel (Chris Hoofnagle, then director of the Information Privacy Programs at the Berkeley Center for Law and Technology), one by defense counsel (Timothy Sparapani, then Facebook's Director of Public Policy), and one by both parties (Larry Magid, CEO of ConnectSafely.org). The Articles also name Scott Kamber and Michael Rhodes to a Board of Legal Advisors tasked with offering nonbinding advice on any matter, including compliance with the settlement agreement.

Several class members and advocates opposed the settlement, some of whom appealed the approval to the Ninth Circuit and then the U.S. Supreme Court. They argued that the settlement was unfair because of the inclusion of a Facebook employee on Digital Trust's board of directors. They also opposed the creation of a new grantmaking entity with the *cy pres* funds because the Foundation had no substantial record of service. A Ninth Circuit panel denied the appeal (with one dissenter).[3] The majority opinion noted that settlement agreements inherently involve give-and-take and that it was unremarkable for Facebook to want to have a role in selecting the fund recipients. The court also had no problem with using *cy pres* funds to establish a new Foundation, especially given that Digital Trust's Articles of Incorporation indicate exactly how the funds would be used and the mission statement advances the privacy interests asserted by the lawsuit. The Supreme Court declined to hear the case, making the 9th Circuit holding final.

Although the settlement was ultimately upheld, it is worth noting that the concept of the Digital Trust Foundation received pointed judicial criticism from high places. Most significantly, Chief Justice Roberts of the U.S. Supreme Court issued a rare "statement" along with the Court's official denial to hear the case.[4] The main thrust of his statement was to indicate that, although he agreed for technical reasons with the decision to forgo review of this case, he hoped to take up a future case that would result in cabining the use of *cy pres* remedies. His statement also took issue with "a number of disconcerting features" of the Foundation: "the fact that a senior Facebook employee would serve on its board, that the board would enjoy nearly unfettered discretion in selecting fund recipients, and that the Foundation—as a new entity—necessarily lacked a proven track record of promoting the objectives behind the lawsuit." Moreover, the dissenting judge on the 9th Circuit panel doubted that any member of the original class would benefit from the settlement.[5] Instead, he foresaw the Foundation serving as a PR win for Facebook and as a way for lawyers on both sides to "serve their interests and pay salaries and consulting fees to persons they choose."

[2] Id.
[3] Lane v. Facebook, Inc., 696 F.3d 811 (9th Cir. 2011).
[4] Marek v. Lane, 571 U.S. 1003 (2013).
[5] Lane v. Facebook, Inc., 696 F.3d 811, 834 (9th Cir. 2011).

Starting Up: November 2013 – May 2014

In November 2013, the Digital Trust Foundation board of directors convened for the first time, with Erin Egan, Chief Privacy Officer at Facebook, replacing Timothy Sparapani in the spot selected by defense counsel. In addition to serving on the board, the directors filled unpaid officer roles, with Hoofnagle acting as President, Egan as Secretary, and Magid as CFO.

Early on, the board agreed to make decisions by consensus. In addition, the members confirmed their mutual intent to treat Digital Trust as a spend-down foundation, with the idea of wrapping up within two years. The board also wanted to make sure that as much of the settlement money as possible ended up the field, so they committed to keeping administrative costs well below those of a typical institutional foundation of this size.

Establishing a Planning Process

The board's first major action was to hire a consultant with philanthropic experience. The board selected Samantha Graff (one of this report's authors), a policy and strategy consultant with a background in the foundation world and in public health law. Process-wise, Graff's role was to serve as a facilitator and project manager, helping the board members do their best thinking and move forward efficiently and effectively. Substantively, Graff brought grantmaking experience to a leadership team whose expertise lay in the topical focus of the Foundation—digital privacy and security—but not the ins and outs of running a foundation. In addition, from her work in public health, she brought a prevention perspective to social problems, which appealed to those directors who wanted the Digital Trust to address privacy as a group interest.

The directors were eager to get the money into the field as quickly as possible, but they also felt a keen responsibility to implement the Foundation's mission in a credible, objective, and impactful way. They saw themselves as accountable to the court that approved the settlement as well as to the privacy field. They wanted to coalesce around a set of strategic grants that would make a meaningful contribution to protecting users' personal information and safety online.

With all of the board's interests in mind, Graff advised the members not to rush toward issuing RFPs, but instead to take some time to clarify their goals, strategy, and operating model. Balancing the desire for speed and efficiency with good grantmaking practices, Graff guided the board through a streamlined planning process.

Defining Program Areas

The planning process kicked off with a productive day-long meeting on January 16, 2014, that laid the groundwork for the substance of the Digital Trust's grantmaking. The board came out of the day with a set of guiding principles for selecting the Foundation's program areas:

1. Ensure broad participation, accounting for the varied interests of stakeholders
2. Give some priority to underserved populations
3. Select goals that are manageable, achievable, and measurable
4. Support research-based interventions
5. Promote not only education but also innovation and structural solutions

The directors also articulated what they saw as the most pressing unmet needs in the privacy field and developed a list of possible program goals to address those needs in the Foundation's grantmaking.

After the January meeting, through conference calls and emails, the directors worked on sorting and prioritizing the list of program goals and fleshing out strategies for achieving those goals. They used a simple template to explore possible program areas that, for each program goal under consideration, called for: (1) identifying the given problem the Foundation was aiming to help solve; (2) defining the gaps that the Foundation was uniquely qualified to fill; (3) describing the impact the Foundation aspired to make; and (4) proposing some possible funding mechanisms. Given that the group wanted to reach consensus about the program areas while meeting the guiding principles established at the January meeting, it took many iterations to find common ground. By May 2014, they had settled on five program areas:

1. Privacy education for youth
2. Understanding socioeconomic status and online privacy and security
3. Assessing, preventing, and addressing digital abuse
4. General funding for sustaining or scaling effective online privacy, safety, and security projects at organizations with demonstrated success in the field
5. Innovation in privacy enhancing technologies

They also had a rough budget and a strategy including one to three conceptual sketches of the types of grants that Digital Trust would give in each program area.

Finding People

The Foundation directors shared a vision of a lean operating model, and at the same time, they felt strongly about engaging high quality personnel and services. This was first expressed in the decision to hire Graff—rather than a brick-and-mortar consulting firm or a full-time executive director—to help launch the Foundation.

As the program areas started taking shape in February, it became clear that Digital Trust would need someone to fulfill the functions of a program officer. After considering various ways to staff this role and exploring several candidates, in March 2014, the board engaged consultant Christine Fry (the second author of this report), who had previously worked with Graff. Fry appealed to the directors because of her complex project management experience and the lucid work plan she proposed for the various threads of activities to be done. They considered it a plus that she had no experience in the privacy field because the board had plenty of subject-

matter expertise to bring to bear, and Fry would add a fresh and objective perspective. Fry agreed to work half time for a year under Graff's guidance to help refine the program area strategies; design and execute the grantmaking process; and develop and implement a plan for communicating on behalf of the Foundation with potential grantees, eventual grantees, and the larger online privacy community.

The board filled additional key functions as follows:

- *Administrative*: Drew Kloss, Hoofnagle's executive assistant at Berkeley Law School, provided light touch administrative support to the Foundation during his off hours.
- *Legal*: Harper & Associates, a well-reputed two-attorney firm, charged less than half the hourly rate of a large law firm to do the basic legal work involved in setting up and running the Foundation.
- *Accounting*: Michael Simmons, a seasoned accountant, was engaged to prepare the Foundation's taxes and 990s.
- *Bookkeeping*: Jenny Brick, a social sector bookkeeper, signed on to set up the Foundation's accounting systems and do monthly bookkeeping.

Setting Up Finances and Operations

Hoofnagle was the Foundation's de facto leader, driving the search and hiring efforts as well as the administrative aspects of getting Digital Trust up and running. Hoofnagle kept Egan and Magid up to date and obtained input and approval from them where appropriate.

In order to keep costs down, Digital Trust had no physical location. The consultants worked remotely in the Bay Area, scheduling occasional in-person check-ins with Hoofnagle. Most board meetings took place via teleconference. The board decided to convene on an as-needed basis, which amounted to seven meetings in the Foundation's first year. Most of the meetings focused on grantmaking, with other business addressed where necessary.

Ensuring Transparency and Accountability

While still working on refining the program areas, the directors took three steps in the spring of 2014 to express their commitment to transparency and accountability: launching a website with a blog; adopting a conflict of interest policy; and hiring an evaluator.

One of Fry's first tasks was to set up a simple website including a blog with periodic updates on the Foundation's activities. The website also included a contact form so the field had a way to reach the Foundation with questions and comments even before the calls for proposals came out.

The board was committed to avoiding any bias or perception of bias in Digital Trust's grantmaking. Therefore, they honed and adopted a rigorous conflict of interest policy that drew

from that of several prominent foundations but that was tailored to address the unique circumstances of the Digital Trust decision-makers.

On Graff and Fry's recommendation, the board decided to engage the highly respected Harder & Company to help develop a basic evaluation plan. Most foundations conduct some form of evaluation,[6] which is often used internally to improve their grantmaking. Grantees commonly complain that they are subject to evaluation requirements by funders but do not benefit from the lessons learned.[7] Given the circumstances under which Digital Trust was created and the fact that it was a spend-down foundation, the board wanted to explore an evaluation approach that provided accountability and transparency to all interested parties and that benefited the grantees and privacy field.

Designing the Grantmaking Process: Summer 2014

Developing Program Area Plans

Fry created a template that she used to flesh out program area plans for the board's consideration. Each plan began with a research memo articulating the problem the Foundation was seeking to address and explaining how and why the Foundation would tackle the problem, citing evidence in support of the given approach. Following the memo was a logic model unpacking the theory of change behind the program area.

Next, each program plan identified the grant portfolio specifications for the program area, including:

- How many grants would comprise the portfolio
- How much money applicants could seek
- How the Foundation would solicit proposals—open vs. invited, and requests for proposals (RFPs) vs. letters of intent (LOIs)
- One or more categories of eligible projects, including mandatory and preferred criteria

Finally, the program area plans provided a list of key organizations working in the space to give the board a sense of the landscape. The directors provided feedback on each draft program area plan, which Fry incorporated into final versions for board approval.

[6] Coffman, J., Beer, T., Patrizi, P., & Heid Thompson, E. (2013). Benchmarking Evaluation in Foundations: Do We Know What We Are Doing? *The Foundation Review*, 5(2), 5.
[7] Buteau, E., & Chu, T. (2011). *Grantees Report Back: Helpful Reporting and Evaluation Processes*, CEP: Data in Action.

Designing the Proposal Process

Given their experience on both the giving and receiving ends of grantmaking, Graff and Fry placed a big priority on researching best practices and designing a streamlined process that provided for responsible due diligence while minimizing administrative burdens on grant applicants.[8]

Digital Trust chose to do open solicitations for all but one project in order to surface the best proposals, including those from unlikely or unknown applicants. The exception was the reporting fellowship focused on understanding socioeconomic status and privacy. Because of the specialized nature of this project, the Foundation identified two highly respected, award winning investigative journalism organizations as the most viable candidates and invited proposals from them. All of the open solicitations were requests for full proposals except for a request for letters of interest issued in the "general funding" program area. Due to the broad requirements of the general funding program area, the board expected a high likelihood of ineligible applications, so it made sense to do some narrowing before requesting full proposals. (In the general funding area, the Foundation ended up receiving 50 letters, inviting 21 proposals, and funding 12.)

As intended, the requests for proposals (RFPs) closely tracked the program area plans. Fry created two standard templates for all applicants to complete: a basic project budget spreadsheet and a form providing a checklist of all required documents and asking for basic organizational information and a project timeline. Each distinct RFP contained:

- A simple statement of the program area goals
- A background memo (based on the research memo from the program area plan) setting forth the evidence and reasoning behind the RFP
- Project requirements and priority criteria
- Evaluation requirements, which sometimes involved complying with simple reporting forms and sometimes mandated that formal evaluations be woven into the project
- A proposal narrative template setting a six-page limit

[8] Resources consulted included: William and Flora Hewlett Foundation. (2012). *Outcome Focused Grantmaking: A Hard-Headed Approach to Soft-Hearted Goals*; Kibbe, Barbara D. et al. (1999). *Grantmaking Basics, A Field Guide for Funders: Reviewing Grant Proposals*. Council on Foundations; Grantmakers for Effective Organizations. *Widening the Pool: Open and Inclusive Grant Competitions*; La Piana Consulting. *Due Diligence Done Well: A Guide for Grantmakers*. Grantmakers for Effective Organizations; La Piana Consulting. (2004). *The Due Diligence Tool For Use in Pre-Grant Assessment*, Grantmakers for Effective Organizations; Brest, P. & Harvey, H. (2008). *Money Well Spent: A Strategic Plan for Smart Philanthropy*. Bloomberg Press; Council on Foundations. (2009). *Essential Skills & Strategies for Grantmakers*.

Core Grantmaking: October 2014 – June 2015

Selecting Grantees

The board decided to stage the RFPs, with the first issued in October. The first grant decisions were made a year and two months after the Foundation's inaugural board meeting. Ultimately, grantees were selected in three board meetings occurring in January, May, and June 2015.

For each RFP, the selection process had four stages. First, Fry cut applicants that failed to meet the basic proposal requirements or to show financial solvency. Next, Fry eliminated proposals that did not align with the Foundation's funding goals—providing short summaries in case the board wanted to revisit any of them. Fry analyzed the remaining proposals using a scoring template based on the project requirements and priority criteria identified in the RFP. Then, Graff facilitated a board meeting at which the directors made funding decisions. They started with a "dot voting" exercise that yielded an initial ranking of proposals, and then they homed in on a slate through discussion. All decisions were made by unanimous consensus except when board members had a clear conflict of interest and recused themselves from decisionmaking. Ultimately, Digital Trust funded 38 of 107 proposals received (36%).

Narrowing the Program Areas

The board initially established five program areas, and the original plan was for the final RFP to focus on the topic of innovation in privacy enhancing technologies, with the possibility of hosting a technology development competition. After much research and consideration of technology-advancing structures such as DARPA challenges, the board decided that the Foundation did not have enough funds to effectively develop technology. The board decided that increasing the Foundation's investments in the first four program areas would have a greater impact than investing a relatively small amount in technology development. The directors came to this realization after reviewing the compelling proposals received in response to the Understanding Socioeconomic Status and Digital Abuse RFPs. Thus, the board expanded the Foundation's investments in these program areas and eliminated the fifth program area.

Securing Grant Agreements

Digital Trust's grant agreements were straightforward. Depending on the length and amount of a grant, disbursements were spread out over three to seven payments, with each payment issued upon approval of a grant report. Grantees filed simple interim and final reports based on templates provided in the Harder evaluation plan. The reports documented grantee deliverables, successes, challenges, and lessons learned. The Foundation required grantees to conduct their own evaluations for two program area strategies (1.1 Implementation and Assessment of Online Privacy Education Programs and 3.2 Understanding Digital Abuse Prevention) and any grants over $200,000.

Monitoring and Winddown: July 2015 – January 2019

Administering the Monitoring Phase

Once all grant agreements had been executed, Fry transitioned out of her role with Digital Trust to focus on other commitments. The board decided to expand Drew Kloss's role to include tracking grantee interim and final reports, issuing payments, and managing grantee correspondence. Graff reviewed grantee reports to ensure compliance, and Hoofnagle approved interim and final payments. While grantees received standardized report forms, they did not all follow the format or complete it as directed. However, Graff reviewed the performance of the grants to ensure there were no concerns.

This extremely lean staffing model resulted in some miscommunications and delays, but it was sufficient to confirm that most grantees were meeting their commitments. Two grantees had their grants terminated early or payments denied due to underperformance. The lean staffing model helped realize the board's goal of minimizing overhead, which ultimately was under 6%, approximately 60% that of peer foundations with similar grantmaking budgets.[9]

Follow-on Grantmaking

By late spring 2015, the Foundation had granted $6.2 million. In 2016, the board approved two supplemental grants: one to Data & Society researcher Amanda Lenhart and one to then-executive director of Data & Society danah boyd. The Lenhart supplement was due to challenges in administering a survey, which resulted in unexpected increased costs. The boyd grant was made to support Data & Society hosting a convening of the low-SES program area grantees.

As of August 2016, the Foundation had a small percentage of its original funds left. Planning conservatively for the costs of wind-down and evaluation, the board decided to divide $300,000 evenly among 12 existing grantees (Figure 1). The decision was based on performance in executing an existing Digital Trust grant, quality of work, and established reputation in the field.

Figure 1. Grantees receiving $25,000 supplemental grants.

ACLU
Center for Democracy & Technology
Center for Digital Democracy
Consumer Federation of America
Electronic Frontier Foundation
EPIC

[9] Comparing to Figure 6: Charitable Administrative Expenses as a Share of Qualifying Distributions, 2007-2009: Family Versus Non-Family, https://foundationcenter.issuelab.org/resources/14077/14077.pdf

Family Online Safety Institute
National Cyber Security Alliance
Privacy Rights Clearinghouse
Internet Keep Safe Coalition (iKeepSafe)
FPF Education and Innovation Foundation
Without My Consent

Selecting an Evaluation Approach

As mentioned above, early on, the board engaged Harder & Company to develop a basic evaluation plan. Harder helped Graff and Fry craft logic models for each program and designed simple interim and final reporting forms for Foundation grantees to use. Harder's plan laid out three options for how to approach evaluation, all of which are commonly-used program evaluation approaches in the social sector.

- Option 1: Grant Monitoring
    - *Approach*: Foundation staff synthesize data collected from grantees through interim and final reports.
    - *Goal*: Address questions related to accountability and potentially extract some lessons for the field from the grantee reports.

- Option 2: Grant Monitoring and Evaluation: The Grantee Perspective
    - *Approach*: Complete everything under Option 1 and add data from grantees collected by an independent evaluator—through a survey, interviews, and an external literature scan.
    - *Goal*: Address questions related to accountability and explore lessons for the field from the perspective of grantees.

- Option 3: Grant Monitoring and Evaluation: The Grantee and Key Leader Perspective
    - *Approach*: Complete everything under Options 1 and 2 and include board and staff member interviews and external stakeholder interviews.
    - *Goal*: Achieve everything under Option 2 as well as exploring board and staff members' views on the grantmaking process, external stakeholders' views on how grantees contributed to the field, and whether the Foundation was an effective way to disseminate settlement funds.

The directors considered the three alternatives and ultimately decided on Option 1 because they thought that there was more to be gained from maximizing the money pushed into the field than expending substantial funds on an independent evaluation. Moreover, as a spend-down foundation, Digital Trust would not exist long enough to monitor the long-term impact of its grantmaking. Downsides of selecting Option 1 included: a reliance on grantee self-reporting with limited external validation; a focus on outputs rather than impact; and a dearth of

information from the field about what might be learned from the Foundation's investments. Furthermore, it is an open question as to whether the value of the work completed was commensurate with the funding spent. However, these are the types of questions that all funders grapple with, even those that invest significantly in evaluation.

Part II of this report summarizes the major outputs of each Digital Trust grant. The summaries are drawn from grantees' interim and final reports.

Shutting Down the Foundation

During the summer of 2017, the board began planning to wind down Digital Trust, as most grants had wrapped up by then. In September 2017, the Foundation re-hired Fry to monitor and close out the remaining grants, update the website with grant results, and dissolve the Foundation. They also asked Graff and Fry to write this final report, which would serve as a record of Digital Trust's work for the privacy and philanthropy fields.

The State of California requires 501(c)3 organizations that intend to dissolve to distribute remaining assets to one or more other 501(c)3 organizations. The board unanimously approved a plan to distribute any remaining funds to Data & Society Research Institute, a nonprofit research organization based in New York that received five grants from the Foundation totaling more than $800,000. Data & Society was chosen because of the organization's exceptionally strong performance as a grantee, both from substantive and administrative standpoints. As of the writing of this report, the exact amount of remaining funds was not yet known, but it was projected to be approximately $75,000.

II. GRANT RESULTS

Based on interim and final grant reports, the Appendix summarizes major outputs of all 38 grants. In addition, Table 1 attempts to roll up grant results into cumulative accomplishments by program area, presenting them alongside the Foundation's original goals for grantmaking. Given variation in types of projects, types of data used to report results, and quality of reporting, these cumulative accomplishments do not represent the entirety of what was achieved by grantees.

Table 1. Grant Result Highlights Aligned with Program Area Goals

The Appendix provides links to many of these projects' outputs.

Program Area	What the Foundation Hoped to Achieve	Grant Result Highlights
1: Privacy Education for Youth	• Increase the privacy resilience of children and teens in the face of complex data-sharing environments • Help children and teens develop skills and resources to protect them in the digital environment throughout life	• At least 345 educators and 3,700 middle and high school students across the country were trained on digital literacy. • 4 digital literacy curricula for middle and high school students were updated or created. 3 of these curricula are free to the public. • Representatives from 40 education technology startups were trained on student privacy laws. • 220 student data privacy stakeholders were convened at the National Student Privacy Symposium to discuss student data privacy requirements. • Several new resources on student privacy were revised or developed and made available for free to the public. • 4 evidence-based media campaigns on digital privacy for youth were developed and launched publicly. • 2 research syntheses on digital literacy of middle and high school students, parents, and educators were developed and made public. • 3 research syntheses of strategies for youth behavior and norm change, each taking a different perspective on the literature, were developed and are pending publication. • 1 public health research center leveraged this opportunity to explore the intersection of digital privacy and public health into an opportunity to collaborate with another digital privacy organization.

		• Another organization is building on this work with a Gates Foundation grant to develop an intervention focusing on technology use in 10-14 year olds.
2: Understanding Socioeconomic Status and Online Privacy and Security	• Understand online privacy and security from the perspectives of low-SES populations • Identify whether, and if so, where a differential approach to online privacy and security protections is needed for low-SES populations • Provide online privacy and security services and information to low-SES populations	• 3 large-scale surveys of low-SES people about digital privacy concerns and practices, 1 exclusively focused on low-SES people living in rural Appalachia were conducted. • At least 10 manuscripts were submitted for publication or published in peer-reviewed journals. • Dozens of presentations of research findings were given at conferences and public events. • A special issue of the International Journal of Communication focused on Privacy at the Margins was edited by one grantee, attracting 44 submissions focused on privacy and marginalized populations. • A field-building workshop was hosted, bringing together researchers focused on digital privacy and low-SES populations.
3: Assessing, Preventing, and Addressing Digital Abuse	• Document the prevalence and severity of various forms of digital abuse • Understand and support digital abuse prevention strategies • Contribute constructively to the digital abuse policy debate	• 2 national representative surveys on digital abuse, 1 focused on Americans 15 and older and the other focused on middle and high school students, were conducted, generating datasets that will be used for years to come. • Secondary analysis of an existing survey dataset was conducted, with a focus on cyberbullying of youth with disabilities, cyberbullying victimization rates by developmental stage, cyberbullying and suicidal ideation, and power imbalance in cyberbullying versus in-person bullying. • Several resources for the general public and parents were produced, and analysis of one of the surveys

		garnered extensive media coverage in the popular press. • At least 10 manuscripts were developed or submitted for publication and more than 20 conference presentations were given. • 2 in-depth legal resources for digital abuse survivors, lawyers, and law enforcement were developed or updated. • 2 services to address digital abuse, one for victims and one for schools, were developed and piloted. • 2 white papers on sextortion raised awareness among federal lawmakers and law enforcement officials about the lack of federal legal protections and data collection for sextortion crimes, resulting in bipartisan legislation being introduced in the House of Representatives and extensive media coverage.
4: General Funding for Promotion of Online Privacy, Safety, and Security	• Support effective existing programs related to online privacy, safety, and/or security • Build capacity of and provide stability for online privacy, safety, and/or security organizations	• 11 consumer education and advocacy organizations and 1 research center were funded. • Online resources and in-person trainings were developed to educate the general public about a range of digital privacy and security issues, including identify theft targeting members of the military, how to make mobile payments safely, privacy and security settings on various websites and platforms, two-factor authentication, and threats posed by Internet and mobile marketplace consumer data tracking systems. • Best practice recommendations were developed and disseminated to influence action by standards bodies, regulators, federal agencies, and internet companies. These recommendations led to a federal government mandate to require all federal websites to move to

		encryption by default, engagement with major companies like Facebook and Palantir on algorithmic fairness, and efforts to educate regulators on protecting financial inclusion and economic mobility in the Big Data era. • Research was conducted on privacy-related legal categorizations such as data versus metadata and parents' knowledge and practices related to protecting their children's privacy online.

III. REFLECTING ON OUR WORK

Without an independent evaluation, it is difficult to comprehensively and credibly document our successes and failures. In the previous two sections, we have attempted to tell the story of Digital Trust in as objective and transparent a manner as possible, with the hope that interested parties can draw their own conclusions about whether the Foundation achieved what it set out to accomplish. For the sake of posterity, we also provide some analysis and reflections below about the success of our operations and about whether the Foundation met its goals.

Regarding the Foundation's operations, in retrospect, we would have advised the board to invest more into overhead or simplify the grant payment and tracking schedules. We supported the board's decision to run a lean operation in order to put as much money as possible into the field. But the limited administrative infrastructure resulted in avoidable problems. Specifically, during the monitoring phase it became clear that the Foundation should have put more resources into grant tracking and record keeping once all of the grants were made and Christine Fry transitioned out. The effects of this included some delayed payments to grantees, periods of delayed communication with grantees, and reports received on incorrect forms or without forms fully completed. This could have been ameliorated either by maintaining a slightly more robust staffing model (which would have meant less money provided in the field) or by reducing the number of scheduled payments and reports.

Adherence to Guiding Principles

As described above, at the first board meeting in 2014, the directors established a set of guiding principles for the Foundation's grantmaking. Here we reflect on whether the Foundation stayed true to these principles:

1. Ensure broad participation, accounting for the varied interests of stakeholders

Digital Trust funded a wide range of organizations, including stalwart advocacy groups, organizations more closely aligned with industry, small start-up organizations, a school district, and several academic research centers. Many of the projects had a national focus, but those focused on specific geographies operated in California, Michigan, New York, North Carolina, Texas, and rural Appalachia.

2. Give some priority to underserved populations

At least one-third of the grant dollars went to projects in Program Area 2: Understanding Socioeconomic Status and Online Privacy and Security. Prior to our grantmaking in this area, this was an under-researched topic, with just a few book-length investigations devoted to it. Now, there are several, well-respected investigators devoting significant research efforts to

low-SES issues. In addition, the board prioritized underserved populations in its grantmaking in other program areas, including digital abuse survivors, youth of color, and veterans.

3. Select goals that are manageable, achievable, and measurable

As summarized above and outlined in detail in the evaluation plan, we believe that we set manageable, achievable, and measurable goals for our grantmaking. We also can reasonably say that our grants made progress towards most of the program area goals in so much as the grantees reported having completed the activities and deliverables specified in their original proposals. For example, a major goal of the Foundation was to educate youth about digital privacy, and we know from grant reports that at least 3,700 youth were directly educated as a result of our grant funds. Although many grantees assessed the immediate impact of these educational efforts through surveys, we cannot evaluate the ultimate effectiveness and reach of these programs as a whole. This is due in part to inconsistent grantee reporting and the decision not to pursue a more robust evauation approach. But it also reflects the challenge all foundations face when it comes to capturing the long-term impact of their grantmaking when their contribution is one of many factors affecting the outcome they are aiming to achieve.

4. Support research-based interventions

A strong theme in our RFPs was a desire to fund research and evidence-based interventions. One third of our grants funded research, while nearly all of our other grants had either an evaluation requirement (direct service grants) or were informed by research (resource development grants). As summarized in Table 1, our grants generated a great deal of knowledge that resulted in several datasets that will be used for years to come, numerous peer-reviewed publications, and dozens of conference presentations.

5. Promote not only education but also innovation and structural solutions

The Foundation funded many educational solutions, from direct education of youth to online self-help resources. Our grantees also produced research and analysis that informed government and the private sector, leading to changes in both policy and practice.

Conclusion

The Digital Trust Foundation demonstrated that *cy pres* funds can be responsibly and effectively disbursed by an expert-led foundation. Digital Trust practiced a culture of accountability by implementing a strategic, consensus-based grantmaking process; adopting a conflicts of interest policy; issuing open RFPs; monitoring grants; and releasing this report for public consumption. Compared to standard *cy pres*, which often results in unsupervised, open-ended gifts to litigants' favored institutions, the Foundation supported diverse organizations with specific agendas in the promotion of education, digital privacy, and online safety.

APPENDIX: GRANT OUTPUT SUMMARIES

Organization	Original Grant Amount	Original Grant Term	Summary of Outputs	Selected Resources and Articles
Notes:	We report the original amount of all grants awarded, not including supplemental awards or early terminations (see main report for more details). We report the original grant term. Many grantees requested and were given no-cost extensions beyond the initial grant term. Summary of Outputs is based on information reported by the grantee in their final report to the Foundation. Selected Resources and Articles is an incomplete list of publicly-available materials created with grant dollars. Several more publications were under peer review or in development as of the writing of this final report.			
Program Area 1.1: Implementation and Assessment of Online Privacy Education Programs				
Fordham University, Center on Law and Information Policy (CLIP)	$120,000	24 months	This grant funded CLIP to recruit and train law student volunteers at Fordham and other schools across the country to educate middle school students about privacy. During the grant term, 51 people trained to teach a privacy education program, and they educated 1,195 students on understanding the importance of privacy and good digital citizenship and the effect that online behavior has on one's reputation, relationships, and future success. CLIP updated the curriculum annually and made it available online on an open source basis. CLIP also expanded the program by reaching out and providing resources through the Educational Leadership Institute for school leaders and admininstrators to teach the curriculum on their own.	https://www.fordham.edu/info/24071/privacy_education
FPF Education and Innovation Foundation	$125,000	24 months	This grant supported the creation of resources, convenings, and activities designed to educated stakeholders on legal uses of student data, opportunities to correct inaccurate data, and ways to increase privacy controls and protections. FPF relaunched its website FERPA|Sherpa, named after the federal law governing student data privacy, in June 2017 with a slew of updated and new resources for parents, schools and districts, ed tech companies, and policy makers. New resources included: The "Parent's Guide to Student Data Privacy," developed with the National PTA and Connect Safely in English and Spanish, to provide families with information about their rights under FERPA and COPPA; and The Educators Guide to Student Data Privacy, developed with Connect Safely to enable teachers to educate themselves about how to evaluate an app or program, and protect a student's personally identifiable information. Convenings included: The National Student Privacy Symposium, which gathered more than 220 industry advocates, privacy experts, and educators in DC to discuss the value of student data, and the requirements for student data privacy; and a Student Privacy Boot Camp at UC Hastings Law School in San Francisco, where about 40 ed tech startups learned about pertinent student privacy laws and their own responsibility to protect student data in partnership with schools. In addition to new resource development and convenings, FPF also partnered with the Houston Independent School District to engage students in all grades in creating videos that address data privacy issues affecting their peer group. Winning videos were posted on FERPA|Sherpa and Houston ISD websites.	http://www.ferpasherpa.org/
Harris County Department of Education	$187,500	14 months	Harris County (Texas) Department of Education developed and implemented a 30-hour online digital literacy training course for teachers and students. The curriculum has four modules: digital citizenship, digital safety and the law, social media use in the classroom, and digital interventions. HCDE deployed the course in the Cypress-Fairbanks Independent School District, a large district in Houston. Eighteen middle school teachers and two district staff were trained, and they rated their overall satisfaction with the curriculum at 3.43 out of 4 points. The teachers then taught the curriculum to 521 middle school students, spending an average of 12.5 hours discussing digital privacy with students over the course of the school year. Limited outcomes data show that teachers increased their digital literacy knowledge and, based on teachers' perception, students have also increase their digital literacy as a result of the curriculum.	

Organization	Original Grant Amount	Original Grant Term	Summary of Outputs	Selected Resources and Articles
Notes:	We report the original amount of all grants awarded, not including supplemental awards or early terminations (see main report for more details). We report the original grant term. Many grantees requested and were given no-cost extensions beyond the initial grant term. Summary of Outputs is based on information reported by the grantee in their final report to the Foundation. Selected Resources and Articles is an incomplete list of publicly-available materials created with grant dollars. Several more publications were under peer review or in development as of the writing of this final report.			
Internet Keep Safe Coalition	$100,000	12 months	This grant supported the expansion of a suite of cloud-based tools aimed at educating the school community about protecting student data and increasing the privacy resilience of children. The grant funded the expansion of professional development learning modules and training videos; updating an incident response tool flowchart for schools investigating digital incidents such as cyberbullying; and adding a privacy matrix to curriculum resources. Internet Keep Safe Coalition conducted train-the-trainer professional development trainings for 100 teachers and administrators and student presentations for 454 students and student leaders (who in turn trained their peers) in Indiana, California, and Washington, DC. The organization also conducted 2 large-scale regional trainings for 167 school and district administrators through the Santa Clara Office of Education and Ventura County Office of Education (California).	http://generationsafe.ikeepsafe.org/
Massachusetts Aggression Reduction Center	$125,524	24 months	This grant supported the revision of middle school and high school digital literacy curricula, with an emphasis on cyberbullying, based on new research into youth digital attitudes and behaviors. The revised curricula were pilot tested at six school locations, training 1,530 students. The curricula are now available on the MARC website, and, as of June 2017, have been requested 96 times by schools reaching a potential total of 46,000 middle and high school students.	https://www.marccenter.org/educators
DPR Educational Services	$100,000	5 months	This grant supported the Digital Ambassadors after-school program in Detroit, which set out to train elementary and middle school students and parents in digital literacy using the Common Sense Education Digital Life 101 curriculum. Each student was trained with the expectation that they would become peer mentors to other students. Seventy-nine students and 16 parents from three schools were trained. Seven instructors at the three schools were also trained to teach the curriulum.	
Program Area 1.2: Online Privacy Campaigns for Youth				
California State University, Northridge	$193,491	15 months	This grant supported focus groups of, surveys of, and interviews with middle-school-aged youth, parents, and educators about young people's digital literacy and behavior. Research findings were used to develop three media campaigns, focused on data brokers, online tracking, and protecting personal information while online. Research findings and media campaigns were presented at five national conferences and peer-reviewed publications were in development at the end of the project.	https://www.youthprivacyprotection.org/
YTH	$150,000	12 months	This grant supported research into teen knowledge, attitudes, and practices related to privacy and safety online and educational website development. YTH produced a 40-page report, “Teen Privacy and Safety Online: Knowledge, Attitudes, and Practices,” summarizing its research. Following the report, YTH developed Between2Screens, a website educating youth around digital safety tips. The website features youth-friendly language around best practices for safety and security online, such as tips for safe gaming, location sharing, and the difference between a public and private profile. Through the website, YTH launched a video challenge designed for U.S. youth, aged 13-17, to share their experiences with digital privacy. The contest received 18 entries and awarded four prizes. More than 100,000 youth were reached during the grant period through the website and social media.	http://between2screens.com/ http://yth.org/research/teen-privacy-safety-online-knowledge-attitudes-practices/

Organization	Original Grant Amount	Original Grant Term	Summary of Outputs	Selected Resources and Articles
Notes:	We report the original amount of all grants awarded, not including supplemental awards or early terminations (see main report for more details). We report the original grant term. Many grantees requested and were given no-cost extensions beyond the initial grant term. Summary of Outputs is based on information reported by the grantee in their final report to the Foundation. Selected Resources and Articles is an incomplete list of publicly-available materials created with grant dollars. Several more publications were under peer review or in development as of the writing of this final report.			
Program Area 1.3: Online Privacy Messaging Best Practices White Paper				
Boston Children's Hospital, Center on Media and Child Health	$49,763	12 months	This grant funded a review of public health literature to identify evidence-based practices that change youth social norms and behavior, with the goal of translating these practices into digital privacy education strategies. Researchers found thousands of articles on youth behavior change and chose to narrow their search to school-based, public health-related interventions. The findings from the literature review will be published in a white paper and peer-reviewed journals. This research also built the capacity of the grantee organization, a public health-oriented organization, to more fully operate in the online civility and digital privacy spaces.	
University of California, Berkeley, Institute of Human Development	$50,000	12 months	This grant supported a review of developmental science models to inform efforts to support youth in navigating complex digital and data-sharing environments. The core outcome of the project was to emphasize the importance of using developmentally-wise approaches to privacy and protection issues, and to highlight the need to develop, refine, and evaluate specific programs based on these principles. At the conclusion of the grant, a manuscript was in development for peer-reviewed publication. Furthermore, this work will be built upon with a grant from the Gates Foundation to develop an intervention focusing on technology use in 10-14-year-old youth.	
University of New Hampshire - Lisa Jones	$49,980	12 months	This grant supported a literature review of youth internet privacy education strategies with a goal of providing recommendations for program development to a range of audiences, including program developers, technology experts, educators, and policy makers. The review emphasized the importance of developing careful program logic when constructing educational or messaging strategies and defining expected outcomes.	
Program Area 2.1: Research into the Privacy Experiences of Low-SES Populations				
Appalachian Center for Resilience Research	$299,718	24 months	This grant funded a study of the online privacy concerns and security practices in a rural, low-SES Appalachian community using a mixed methods approach that included focus groups, interviews, and a large-scale survey. It was the first study of technology in this rural, low-SES community. The study found that as crime moves increasingly online, cyber-victimization is an increasingly important component of the overall burden of victimization. The study identified a wide range of privacy violations that can happen online as well as certain basic safety practices associated with lower victimization rates. Grantees produced four research papers under various stages of review at the time of reporting, six conference presentations, and four briefs for publication in Dr. Hamby's Psychology Today blog and submitted to local media.	

Organization	Original Grant Amount	Original Grant Term	Summary of Outputs	Selected Resources and Articles
Notes:	We report the original amount of all grants awarded, not including supplemental awards or early terminations (see main report for more details). We report the original grant term. Many grantees requested and were given no-cost extensions beyond the initial grant term. Summary of Outputs is based on information reported by the grantee in their final report to the Foundation. Selected Resources and Articles is an incomplete list of publicly-available materials created with grant dollars. Several more publications were under peer review or in development as of the writing of this final report.			
Data & Society Research Institute - danah boyd	$141,421	12 months	This grant funded qualitative research—including focus groups and youth peer interviews—on the language and framing of privacy issues among low-SES teens and young adults. Grantees produced three articles. This research inspired grantees to host a field-building workshop, funded with a supplemental DTF grant, where several recipients of DTF grants on low-income individuals and privacy presented their research and received feedback. D&S thus gathered and seeded a network of researchers working on this emerging area of inquiry. To continue such field-building, D&S has organized a special issue of the International Journal of Communication on "Privacy at the Margins," which attracted 44 submissions on a range of topics to do with privacy and understudied populations. Additional offshoots of this work have included media outreach, recommendations for policymakers, blog posts, and Alice Marwick's contract for a book tentatively titled "Hidden: Networked Privacy, Social Media, and Those Left Out," which will leverage the data collected for this project into a broader argument about the disparate impact of privacy violations on marginalized populations.	Marwick, A., Fontaine, C., & boyd, D. (2017). "Nobody Sees It, Nobody Gets Mad": Social Media, Privacy, and Personal Responsibility Among Low-SES Youth. Social Media+ Society, 3(2), 2056305117710455. https://journals.sagepub.com/doi/abs/10.1177/2056305117710455 Marwick, A. & boyd, D. (2018)."Privacy at the Margins." International Journal of Communication, 12, 1157–1165 https://ijoc.org/index.php/ijoc/article/view/7053/2293 Pitcan, M., Marwick, A. & boyd, D. (2018). "Performing a Vanilla Self: Respectability Politics, Social Class, and the Digital World." Journal of Computer-Mediated Communication, Volume 23, Issue 3, 1, 163–179 https://doi.org/10.1093/jcmc/zmy008https://academic.oup.com/jcmc/article/23/3/163/4962541
Data & Society Research Institute - Karen Levy	$74,976	12 months	This grant funded qualitative research on low-wage workplace issues in the retail and agricultural sectors. Regarding retail, grantees examined customer data tracking practices used in the industry and their implications for the management of low-wage workers. Research resulted in a proposal for a new framework for analyzing surveillance that more fully accounts for the impacts of surveillance in modern life, particularly with respect to economic effects, and recommendations for practitioners and industry to address ways in which the use of refractive surveillance can undermine or support workers' economic and social outcomes. Grantees' work on refractive surveillance has led them to conceptualize a new research project on privacy interdependencies. Regarding agriculture, grantees produced a case study based on three fieldwork trips (available on SSRN) that spawned a new research agenda for them on the topic that will be supported by two further grants. As of the final reporting date, grantees had presented findings from their work at 12 events, including both academic conferences and events open to the public.	Levy, K., & Barocas, S. (2018). Refractive surveillance: Monitoring customers to manage workers. International Journal of Communication, 12, 1166-1188 https://ijoc.org/index.php/ijoc/article/viewFile/7041/2302 Barocas S. & Levy K. (2018). What Customer Data Collection Could Mean for Workers https://hbr.org/2016/08/the-unintended-consequence-of-customer-data-collection

Organization	Original Grant Amount	Original Grant Term	Summary of Outputs	Selected Resources and Articles
Notes:	We report the original amount of all grants awarded, not including supplemental awards or early terminations (see main report for more details). We report the original grant term. Many grantees requested and were given no-cost extensions beyond the initial grant term. Summary of Outputs is based on information reported by the grantee in their final report to the Foundation. Selected Resources and Articles is an incomplete list of publicly-available materials created with grant dollars. Several more publications were under peer review or in development as of the writing of this final report.			
Data & Society Research Institute - Mary Madden	$270,622	12 months	This grant supported a national survey of American adults with an oversample of low-SES respondents aimed at understanding the everyday privacy and security-related behaviors of low-SES adults and seeking to answer key questions that can ground the policy conversations and debates. Grantees published a Washington University Law Review article that was nominated for the Future of Privacy Forum's Privacy Papers for Policymakers award and was on several SSRN Top Ten lists. Grantees also produced a 124-page report offering the first in-depth analysis of the privacy and security experiences of low- socioeconomic-status populations in the United States. The PI presented and discussed survey findings in many symposiums, conferences, and workshops and has engaged around the findings with several government agencies including the NYC Mayor's Office of Digital Innovation, DHS, and FTC.	Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty, and Big Data: A matrix of vulnerabilities for poor Americans. Wash. UL Rev., 95, 53 https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6265&context=law_lawreview Madden, M. (2017) "Privacy, Security and Digital Inequality: How Technology Experiences and Resources Vary by Socioeconomic Status, Race, and Ethnicity," Data & Society Research Institute. https://datasociety.net/pubs/prv/DataAndSociety_PrivacySecurityandDigitalInequality.pdf
New America	$703,600	36 months	This grant funded a national representative survey and a participatory research project — the Our Data Bodies (ODB) Project — in partnership with grassroots organizations in Charlotte, Detroit, and LA, exploring the nature and experience of digital privacy and "data rights" of adult low-income people in the U.S. As of publication of this report, the grantee was wrapping up their work and writing their final grant report.	
Program Area 2.2: Providing Online Privacy and Security Services and Information to Low-SES People (no grants awarded)				
Program Area 2.3: Journalism Fellowship Focused on Socioeconomic Status and Online Privacy and Security				
Center for Investigative Reporting	$300,000	24 months	This grant funded a fellowship for a reporter to investigate the privacy experience of low-SES people and where a differential approach to privacy protections might be needed. CIR wrote several articles and blog posts and engaged in various forms of outreach regarding the CalGang database, revealing the privacy implications, particularly for low-SES communities, of the use of surveillance techologies by law enforcement.	https://www.revealnews.org/blog/california-state-auditor-rampant-flaws-in-gang-database/ https://www.revealnews.org/episodes/update-eyes-on-cops/
Program Area 3.1: Understanding Digital Abuse Prevalence				

Organization	Original Grant Amount	Original Grant Term	Summary of Outputs	Selected Resources and Articles
Notes:	We report the original amount of all grants awarded, not including supplemental awards or early terminations (see main report for more details). We report the original grant term. Many grantees requested and were given no-cost extensions beyond the initial grant term. Summary of Outputs is based on information reported by the grantee in their final report to the Foundation. Selected Resources and Articles is an incomplete list of publicly-available materials created with grant dollars. Several more publications were under peer review or in development as of the writing of this final report.			
Data & Society Research Institute - Amanda Lenhart	$352,520	12 months	This grant funded a nationally representative landline and mobile phone survey of 3,002 Americans ages 15 years and older to quantify the prevalence of cyberstalking and digital domestic violence, the extent to which people witness others' abusive behavior online, and how online privacy behavior may relate to and even protect against online abuse. The study found that nearly half of American internet users have experienced digital abuse and three-quarters have witnessed it. The results were published in four products for different audiences, including parents, policymakers, and researchers. The research garnered extensive media attention, including the Washington Post, The Atlantic, Esquire, Yahoo News, Business Insider, PC Mag, SFgate, TIME, RT, AFP, Fox News, Teen Vogue, and Newsweek.	https://datasociety.net/blog/2017/01/18/online-harassment-digital-abuse/
University of New Hampshire, Crimes Against Children Research Center - Kimberly Mitchell	$106,259	12 months	This grant funded in-depth secondary data analysis of the Technology-Harassment Victimization (THV) Survey and development of a series of reports, fact sheets, and presentations focused on (1) cyberbullying of youth with disabilities, (2) differences in cyberbullying victimization rates and characteristics across developmental stages including young adolescents, older adolescents, and young adults, (3) the relationship between cyberbullying and suicidal ideation, (4) the role of power imbalance in online harassment and cyberbullying experiences versus in-person bullying. The research resulted in at least five manuscripts under review or in development, six conference presentations, and three resources for parents and clinicians.	Wells, M., Mitchell, K. J., Jones, L. M., & Turner, H. A. (n.d.). Peer harassment among youths with different disabilities: impact of harassment online, in person, and in mixed online and in-person incidents. Children & Schools. https://doi.org/10.1093/cs/cdy025 Mitchell, K. J., Jones, L. M., & Turner, H. A. (2017). Past year technology-involved peer harassment victimization and recent depressive symptoms and suicide ideation among a national sample of youth. Journal of Interpersonal Violence, 886260517748413. https://doi.org/10.1177/0886260517748413 http://unh.edu/ccrc/internet-crimes/Pamphlet%20suicide%20printable%20(final).pdf http://unh.edu/ccrc/internet-crimes/Suicide%20Brief%20(final)%20(002).pdf

Organization	Original Grant Amount	Original Grant Term	Summary of Outputs	Selected Resources and Articles
Notes:	We report the original amount of all grants awarded, not including supplemental awards or early terminations (see main report for more details). We report the original grant term. Many grantees requested and were given no-cost extensions beyond the initial grant term. Summary of Outputs is based on information reported by the grantee in their final report to the Foundation. Selected Resources and Articles is an incomplete list of publicly-available materials created with grant dollars. Several more publications were under peer review or in development as of the writing of this final report.			
University of Wisconsin-Eau Claire	$188,776	12 months	This grant funded one of the largest nationally-representative surveys of middle and high school students to date (over 5,700 respondents), examining national prevalence, frequency and scope of cyberbullying and electronic dating violence. Apart from descriptive findings by age, gender, grade, and other important demographics, analysis will examine contributing factors to perpetration and victimization, as well as the negative outcomes that stem from cyberbullying participation as an aggressor or a target. As of the end of the grant term, findings had been presented at 15 conferences and meetings, shared on the Cyberbullying Research Center website, and submitted to five peer-reviewed journals. Researchers intend to further mine the dataset, producing more publications, presentations, and possibly a book.	Hinduja, S., & Patchin, J. W. (2018). Connecting adolescent suicide to the severity of bullying and cyberbullying. Journal of School Violence, 1–14. https://doi.org/10.1080/15388220.2018.1492417 Patchin, J. W., & Hinduja, S. (2018). Sextortion among adolescents: results from a national survey of u. S. Youth. Sexual Abuse, 107906321880046. https://doi.org/10.1177/1079063218800469 Hinduja, S., & Patchin, J. W. (2017). Cultivating youth resilience to prevent bullying and cyberbullying victimization. Child Abuse & Neglect, 73, 51–62. https://doi.org/10.1016/j.chiabu.2017.09.010 Patchin, J. W., & Hinduja, S. (2017). Digital self-harm among adolescents. Journal of Adolescent Health, 61(6), 761–766. https://doi.org/10.1016/j.jadohealth.2017.06.012
Program Area 3.2: Understanding Digital Abuse Prevention				
National Center for Missing and Exploited Children (NCMEC)	$75,000	12 months	This grant funded dissemination and evaluation of the NetSmartz Student Project Kit, which empowers middle and high school students to educate their peers and younger students about online safety and digital citizenship issues. NCMEC received feedback from 149 users, nearly all of whom expressed satisfaction with the kit. Updates to the kit were made based on feedback, and the kit was also translated into Spanish.	https://www.netsmartz.org/studentkit
Program Area 3.3: Supporting Digital Abuse Victims				
Hollaback!	$120,000	12 months	This grant contributed to the development, marketing, and launch of HeartMob, a platform where victims can safely report their digital abuse and volunteers can respond. The goal of the project is to provide real time support to individuals experiencing digital abuse, and to ensure individual's safety, security, and equality online. In addition to launching the platform, the Hollaback team was able to leverage its expertise and connections to launch a consulting service for online media companies to provide a revenue stream for HeartMob.	https://iheartmob.org/

Organization	Original Grant Amount	Original Grant Term	Summary of Outputs	Selected Resources and Articles
Notes:	We report the original amount of all grants awarded, not including supplemental awards or early terminations (see main report for more details). We report the original grant term. Many grantees requested and were given no-cost extensions beyond the initial grant term. Summary of Outputs is based on information reported by the grantee in their final report to the Foundation. Selected Resources and Articles is an incomplete list of publicly-available materials created with grant dollars. Several more publications were under peer review or in development as of the writing of this final report.			
National Network to End Domestic Violence (NNEDV)	$195,000	36 months	This grant funded updates and additions to a comprehensive online toolkit to help domestic violence survivors understand (1) how they can be safe and secure online, (2) what laws might protect them, and (3) what their legal rights are when they experience abuse online or through technology. NNEDV updated WomensLaw.org with information about federal and state statutes related to technology-facilitated abuse, plain-language explanations of technology-facilitated abuse, and information about civil and criminal remedies for survivors of technology-facilitated abuse. The grant also supported technical assistance to survivors through the WomensLaw.org email hotline.	https://www.womenslaw.org/about-abuse/abuse-using-technology
Net Family News, Inc.	$175,000	6 months	This grant funded the pilot launch of a social media helpline for schools in the state of California during the 2015-16 school year. The helpline was subsequently expanded to Washington and Georgia. Helpline staff have assisted dozens of school staff on social media-related isses, including cyberbullying and sharing of inappropriate content, and independent evaluation has found widespread satisfaction among helpline users. Net Family News has also created case studies based on common issues. The helpline is now available as a low-cost subscription service available to schools nationwide.	https://socialmediahelpline.com/
The Brookings Institution	$188,362	12 months	This grant supported research to define sextortion as a crime and quantify how many people it affects. Researchers then made federal legislative recommendations to better address sextortion. As a result of this work, then-Senator Barbara Boxer (CA) sent a letter to the Department of Justice asking the agency to begin tracking sextortion crimes. Bipartisan legislation to prevent sextortion was also introduced in the House of Representatives as a result of this research. The research reports were covered by several major media outlets, including New York Times, The Atlantic, CNN, Huffington Post, San Francisco Chronicle, NPR, and ABC News. Also as result of this research, YouTube removed a collection of videos on its site that provided instructions on how to commit sextortion.	https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/ https://www.brookings.edu/research/closing-the-sextortion-sentencing-gap-a-legislative-proposal/

Organization	Original Grant Amount	Original Grant Term	Summary of Outputs	Selected Resources and Articles
Notes:	We report the original amount of all grants awarded, not including supplemental awards or early terminations (see main report for more details). We report the original grant term. Many grantees requested and were given no-cost extensions beyond the initial grant term. Summary of Outputs is based on information reported by the grantee in their final report to the Foundation. Selected Resources and Articles is an incomplete list of publicly-available materials created with grant dollars. Several more publications were under peer review or in development as of the writing of this final report.			
Without My Consent	$199,810	24 months	This grant supported the development of a 50-state database of legal information about civil and criminal remedies for victims of nonconsensual porn, a toolkit on legal strategies for combatting sharing of nonconsensual porn in court, and a half-day training workshop curriculum for lawyers on nonconsensual porn law. The online resources have been promoted in popular media, and the training workshop has been presented to law enforcement and law schools.	https://withoutmyconsent.org/50state https://withoutmyconsent.org/resources
Program Area 4: General Funding for Promotion of Online Privacy, Safety, and Security				
ACLU	$100,000	12 months	This grant supported three activities. First, the ACLU enhanced consumer privacy and security by educating the general public. Through blog posts, panels, an op ed, and hundreds of media appearances, ACLU privacy advocates reached a huge swath of the general public and decision-makers and observed that the media and public are both showing a greater interest in technology issues and in individuals' capacity to take steps to protect themselves. The ACLU also released an updated business primer, "Privacy & Free Speech: It's Good for Business." The debut included a new website that received over 1,700 visits in its first two weeks; the distribution of 3,500 digital copies and 300 hard copies; and direct engagement with several Internet giants. The ACLU's advocacy around the toolkit resulted in: implementation of encryption by default on dozens of government inspector general sites; a government mandate to require all federal websites to move to encryption by default; a move to encryption by default by the Washington Post and other news organizations; the first transparency reports from T Mobile and Amazon.com; and a changed in policy at the White House that stops the practice of sending prospective visitors' social security numbers over unencrypted email. The third activity was advocating in front of standards bodies and in administrative proceedings, helping to advance concrete solutions to privacy, security, and safety risks in the internet backbone. This included helping to identify serious vulnerabilities in a proposed anti-surveillance browser plugin and experimental transport layer network protocol; helping to secure two previously-unencrypted codebases important to Domain Name System (DNS) privacy; helping to conceive a patch to make DNS requests and responses less vulnerable to privacy-diminishing traffic analysis; and contributions to the upcoming release of TLS 1.3.	Privacy and Free Speech: It's Good for Business (toolkit): https://www.itsgoodfor.biz/ https://www.washingtonpost.com/news/the-switch/wp/2016/02/29/the-technology-at-the-heart-of-the-apple-fbi-debate-explained/?utm_term=.774b532edea3 https://www.aclunc.org/blog/take-back-control-your-online-identity https://www.aclunc.org/blog/it-s-new-year-here-are-six-digital-privacy-resolutions-keep
Center for Democracy & Technology	$200,000	12 months	This grant supported two new projects of CDT's Privacy and Data Project, one on algorithmic fairness and one on workplace privacy. CDT researched concepts in algorithmic fairness and workplace privacy, analyzed the complex legal and policy landscape around these issues, and convened a broad range of stakeholders to develop best practices and common principles on key concerns. Activities included convenings of the Internet Privacy Working Group and the Health Privacy Working Group and collaboration on special projects; one-on-one dialogue and special projects with key stakeholders across sectors (e.g. Facebook, Nielsen, and Palantir); research and production of guidance documents, rubric, and white paper; numerous workshops and conference presentations (including at the Amsterdam Privacy Conference, the Privacy Law and Scholars Conference, and the Civil Rights and Privacy Table); earned media coverage; and increased social media outreach.	https://cdt.org/files/2016/06/CDTWorkplacePrivacyWhitePaper-Final.pdf https://cdt.org/insight/digital-decisions-policy-tools-in-automated-decision-making/ https://cdt.org/blog/with-workplace-privacy-have-a-policy-and-follow-the-policy/

Organization	Original Grant Amount	Original Grant Term	Summary of Outputs	Selected Resources and Articles
Notes:	We report the original amount of all grants awarded, not including supplemental awards or early terminations (see main report for more details). We report the original grant term. Many grantees requested and were given no-cost extensions beyond the initial grant term. Summary of Outputs is based on information reported by the grantee in their final report to the Foundation. Selected Resources and Articles is an incomplete list of publicly-available materials created with grant dollars. Several more publications were under peer review or in development as of the writing of this final report.			
Center for Digital Democracy	$50,000	12 months	This grant helped support the development of several journal articles and conference presentations exposing the privacy implications for children of Big Data and targeted marketing and outlining policy and regulatory opportunities to allow consumers to regain a measure of control over their personal data online. Research findings were presented at the International Communication Association conference, the National Academy of Sciences' conference on "Digital Media and Developing Minds," and the Amsterdam Privacy Conference.	Montgomery, K. (2015). Childrens Media Culture in a Big Data World. Journal of Children and Media, 9(2), 266-271 https://www.tandfonline.com/doi/abs/10.1080/17482798.2015.1021197?journalCode=rchm20 Montgomery, K. C. (2015). Youth and surveillance in the Facebook era: Policy interventions and social implications. Telecommunications Policy, 39(9), 771-786 https://www.sciencedirect.com/science/article/abs/pii/S0308596114001955 Chester J. & Montgomery, K. Youth Privacy in the Big Data Era, in https://www.routledge.com/International-Handbook-of-Media-Literacy-Education/De-Abreu-Mihailidis-Lee-Melki-McDougall/p/book/9781138645509
Consumer Credit Counseling Service of Rochester	$41,239	36 months	This grant funded the development and delivery of 13 online privacy training workshops for military members pre-deployment and after returning from service—in part addressing their unique risk for identity theft and scammers given their long absences. The first seven trainings reached 267 people, and post-test results from early trainings showed a 26% improvement in knowledge scores. Grantees presented the program model at The Society for Financial Education and Professional Development conference and in three webinars for veterans services agencies around the country.	https://www.cccsofrochester.org/id-theft-and-online-safety-for-military

Organization	Original Grant Amount	Original Grant Term	Summary of Outputs	Selected Resources and Articles
Notes:	We report the original amount of all grants awarded, not including supplemental awards or early terminations (see main report for more details). We report the original grant term. Many grantees requested and were given no-cost extensions beyond the initial grant term. Summary of Outputs is based on information reported by the grantee in their final report to the Foundation. Selected Resources and Articles is an incomplete list of publicly-available materials created with grant dollars. Several more publications were under peer review or in development as of the writing of this final report.			
Consumer Federation of America	$125,000	12 months	This grant supported the creation of accessible, objective educational materials for consumers about how to make mobile payments safely and confidently. The materials, viewable in one central link on CFA's website, include: the comprehenive Guide to Protecting Your Privacy Security When Making Mobile Payments; two ready-to-use news articles; a video; two blogs; and earned media. The materials were finalized and released a week before the end of the grant period, making it difficult to report on their reach and impact, but CFA did report a few early number. For example, CFA sent information about the materials to 280 member consumer organizations and 34 banks and credit unions. The first ready-to-use news article generated 2,356 articles with a readership of 848,000. A radio media tour included interviews with 14 stations with total impressions of over 20 million.	https://consumerfed.org/mobilepayments/
Electronic Frontier Foundation	$100,000	12 months	This grant funded a new staff member at the Digital Privacy Training and Activism project, which educates users about privacy and security settings on various websites, apps, and platforms. This staff person authored a series of step-by-step posts ("12 Days of 2FA") on how to enable two-factor authentication on several of the most popular platforms and apps. These and other blog posts about privacy and security issues reached nearly 400,000 people. Also, a video tutorial and accompanying blog post about privacy settings on Facebook gained nearly 15,000 page views in its first two days live.	https://www.eff.org/deeplinks/2016/12/12-days-2fa-how-enable-two-factor-authentication-your-online-accounts

Organization	Original Grant Amount	Original Grant Term	Summary of Outputs	Selected Resources and Articles
Notes:	We report the original amount of all grants awarded, not including supplemental awards or early terminations (see main report for more details). We report the original grant term. Many grantees requested and were given no-cost extensions beyond the initial grant term. Summary of Outputs is based on information reported by the grantee in their final report to the Foundation. Selected Resources and Articles is an incomplete list of publicly-available materials created with grant dollars. Several more publications were under peer review or in development as of the writing of this final report.			
EPIC	$100,000	24 months	This grant helped expand EPIC's Consumer Privacy Project—strengthening its web presence, improving outreach, bringing important privacy matters to the FTC's attention, supporting the Consumer Privacy Bill of Rights, educating the media about privacy issues, and remaining an advocate for consumer privacy. Deliverables included a journal article, a series chapter, and the EPIC Anthology.	Rotenberg, M., Scott, J., & Horwitz, J. (Eds.). (2015). Privacy in the modern age: The search for solutions. New Press, The. https://www.epic.org/privacy-book/ Rotenberg M., Jacobs D. (2016) Enforcing Privacy Rights: Class Action Litigation and the Challenge of cy pres. In: Wright D., De Hert P. (eds) Enforcing Privacy. Law, Governance and Technology Series, vol 25. Springer, Cham https://www.springer.com/us/book/9783319250458 Rotenberg, M. ,Urgent Mandate, Unhurried Response:, European Data Protection Law Review, Volume 3, Issue 1 (2017), pp. 47 – 70, DOI: https://doi.org/10.21552/edpl/2017/1/8
Family Online Safety Institute	$100,000	12 months	This grant supported the next stage of a longitudinal study focusing on parents' hopes, fears, and actions (e.g., use of parental controls, privacy settings, and reporting mechanisms) regarding their children's online behaviors. FOSI held three focus groups and conducted an online survey of 589 parents of children aged 6-17. The final report was launched at the FOSI Annual Conference, which was accompanied by a research presentation (attended by 400), press release (found on 280 websites), and the posting of findings on the FOSI website and on social media. The launch resulted in a large press pickup, including major news outlets, and FOSI continued to distribute the report at events, meetings, parent nights, and presentations (reaching approximately 6,000 people) in 2016. FOSI plans to use the study findings to create resources for parents and policymakers aimed at making the online world safer for children.	https://www.fosi.org/policy-research/parents-privacy-technology-use/
National Cyber Security Alliance	$150,000	24 months	This grant supported activities of STOP. THINK. CONNECT., which is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the general public to be safer and more secure online. NCSA updated a tip sheet, hosted seven Twitter chats (two of which had potential reach of 856,555 and 1.4 million), posted at least five articles/blogs per week, and conducted a survey to gauge public awareness of the campaign. NCSA shared campaign resources with over 660 partners who use the campaign's non-proprietary materials (and in some cases branding) to spread awareness about the importance of privacy and security.	https://www.stopthinkconnect.org/resources

Organization	Original Grant Amount	Original Grant Term	Summary of Outputs	Selected Resources and Articles
Notes:	We report the original amount of all grants awarded, not including supplemental awards or early terminations (see main report for more details). We report the original grant term. Many grantees requested and were given no-cost extensions beyond the initial grant term. Summary of Outputs is based on information reported by the grantee in their final report to the Foundation. Selected Resources and Articles is an incomplete list of publicly-available materials created with grant dollars. Several more publications were under peer review or in development as of the writing of this final report.			
New York University, Information Law Institute	$125,000	24 months	This grant supported a research fellow and RA to develop a paper studying formalistic legal categorizations—e.g., data vs. metadata and content vs. non-content—and providing recommendations for a new paradigm. The authors presented versions of the paper at the European Privacy Law Scholars Conference, the Oxford Internet Institute (where workshop attendants included representatives from the European Parliament), Ohio State University's Moritz College of Law (which dedicated a one-day symposium exclusively to the research findings), and the Privacy Law Scholars Conference. The paper has been accepted for publication with I/S: A Journal of Law and Policy for the Information Society.	http://www.law.nyu.edu/centers/ili/metadataproject
Privacy Rights Clearinghouse	$250,000	26 months	This grant supported PRC's development and launch of a completely new website that is mobile responsive and provides many navigation options. The complaint submission and question portal is now easier to use and allows users to submit complaints without providing personal information. PRC also published easy-to-share "quick tips" for many of their subject areas; several graphics; three comprehensive infographics on topics that are common areas of concern and confusion; a new blog; and updates of its existing consumer guides. The grant also allowed PRC to hire an outreach coordinator who helped grow PRC's social media presence.	https://www.privacyrights.org/
US PIRG	$100,000	24 months	This grant enabled US PIRG to scale up an existing project evaluating the development of Internet and mobile marketplace consumer data tracking systems; measuring these practices against existing protections and their compliance with the Code of Fair Information Practices; educating consumers, regulators, other policy advocates, enterprises and other stakeholders about threats to privacy posed by the practices; and proposing solutions to regulators, enterprises, and consumers. In particular, the project focused on Big Data and its impacts on financial inclusion and economic mobility. US PIRG held three convenings, published four reports, submitted detailed regulatory comments on at least five occasions, and updated the consumer tips section of its website with better content and a mobile-friendly interface. The project reached more than 1.5 million consumers via literature distribution, and hundreds of thousands more have visited the website. The organization worked in coalition with major national partners, sharing research and tips and communicating regularly with regulators such as the Consumer Financial Protection Bureau.	https://uspirgedfund.org/reports/usf/why-you-should-get-security-freezes-your-information-stolen http://consumertips.uspirg.org/ https://uspirgedfund.org/issues/usf/digital-data-and-consumer-protection-ensuring-fair-and-equitable-financial-marketplace