New York University & Library Freedom Project: Privacy in Libraries (RE-95-17-0076)

Abstract

New York University (NYU), in partnership with the Library Freedom Project (LFP), a nonprofit organization fiscally sponsored by the Tor Project, Inc., seeks a two-year Laura Bush 21st Century Librarian project grant to facilitate the use of privacy tools in libraries and their communities through the development of a privacy-focused train-the-trainer program for librarians, which we will call the Library Freedom Institute (LFI). Building on their successful shorter programs, the project team will construct an extensive curriculum and use it to train 40 geographically dispersed Privacy Advocates, who can then serve as nodes of expertise in their regions by conducting workshops for community members and helping their own libraries become more privacy conscious.

With almost weekly revelations of massive privacy attacks (on email providers, health care companies, governmental agencies, political campaigns, and other targets, including libraries), the public has developed a heightened awareness of the vulnerability of their private information. For marginalized people, the Internet is particularly hostile; Edward Snowden's revelations about overbroad government surveillance, for example, showed that immigrants and Muslims are frequent targets. Data-driven advertising builds upon algorithmic bias to market exploitative products directly to consumers identified as economically disadvantaged. Elderly people lacking access to quality computer education are more likely to be the victims of fraud and identity theft.

Recent headlines confirm the nature of the problem. Vice Media's *Motherboard* recently proclaimed, "Digital Surveillance is Class Warfare," citing a Data & Society Research Institute study that demonstrated greater reliance on smartphones for Internet browsing among poor families relative to wealthier ones—a troubling discovery, given that mobile phone usage is more vulnerable to surveillance than is browsing activity on the average laptop (Jordan Pearson, May 15, 2017).

Public libraries serve everyone, so privacy attacks on the most vulnerable members of our communities should be a serious cause for alarm. Moreover, even the most powerful have been hit by privacy attacks (the Pentagon, the Democratic National Committee), so Internet privacy should be everyone's concern. What's more, libraries recognize the relationship between privacy and intellectual freedom, and privacy has been a key element in the American Library Association's Code of Ethics since decades before the first message was sent over the Internet. Librarians need practical, actionable, 21st Century skills to turn our ethics into reality.

The LFI will cultivate 40 Privacy Advocates, teaching them skills to make privacy a procedural and technical reality in their libraries. Over a six-month course, project staff and guest trainers will teach our Advocates how to lead privacy-focused computer classes at several levels: how to install, troubleshoot, and maintain privacy software on both patron machines and library public workstations; how to teach their own train-the-trainer workshops to other librarians in their regions; how to approach members of their community about privacy concerns; and how to use their new roles as Privacy Advocates to influence policy and infrastructure. During a two-year project timeline, we will plan and run a pilot iteration of the LFI, analyze it, make revisions to the curriculum, offer a full-scale LFI to a larger cohort of librarians, and evaluate the full program.

Library Freedom Institute will be the only professional development program of its kind for librarians, addressing a demonstrable community need for privacy literacy, and turning libraries into privacy-protective community anchors in their regions. This project has the potential to impact library practices for years to come, as we are training librarians to teach others what they have learned. We anticipate three tiers of beneficiaries: the Privacy Advocates themselves, who will gain a unique and in-demand skillset that will help them in their library work and beyond; patrons of the Privacy Advocates' libraries, who will be able to learn a range of meaningful new privacy practices in the trusted space of their local library; and other librarians throughout the country, who can receive direct trainings and other support from their regional Privacy Advocate. Since this project will produce a dispersed network of privacy specialists in libraries, its impact will be wide-ranging, long-lasting, and sustainable.

Privacy in Libraries: Partnership between New York University and Library Freedom Project

New York University (NYU), in partnership with the Library Freedom Project (LFP), seeks a two-year Laura Bush 21st Century Librarian project grant to facilitate the use of practical privacy tools in libraries and their communities through the development of a privacy-focused train-the-trainer program for librarians, which we will call the Library Freedom Institute (LFI). Building on their successful shorter training programs, the project team will construct an extensive curriculum and use it to train 40 geographically dispersed Privacy Advocates, who can then serve as nodes of expertise in their regions by conducting training workshops for community members and helping their own libraries become more privacy conscious.

1. Statement of Need

With almost weekly revelations of massive privacy attacks (on email providers, health care companies, governmental agencies, universities, political campaigns, election officials, and other targets, including libraries), the public has developed a heightened awareness of the vulnerability of their private information. For marginalized people, the Internet is particularly hostile; Edward Snowden's revelations about overbroad government surveillance, for example, showed that immigrants and Muslims are frequent targets. The elderly and those with poor English skills are often the victims of fraud and identity theft. Data-driven advertising builds upon algorithmic bias to market exploitative products, such as subprime loans, directly to those consumers identified as economically disadvantaged. Elderly people, often lacking access to high-quality computer education, are more likely to report feeling insecure when they go online. A Pew research report from 2015 showed that those over 50 are much less likely than younger people to take active measures to protect their privacy and security.[1]

Major headlines make clear the nature of the problem. A recent column in the *New York Times Magazine* argued that while the extremely wealthy can pay to ensure their privacy, as Facebook's CEO Mark Zuckerberg did when he bought up the houses surrounding his own property, the rest of us must tolerate monetization of our personal information in exchange for basic digital services.[2] Vice's *Motherboard* blog, mincing no words, proclaimed, "Digital Surveillance is Class Warfare," citing a Data & Society Research Institute study that demonstrated greater reliance on smartphones for Internet browsing among poor families relative to wealthier ones—a troubling discovery, given that mobile phone usage is more vulnerable to surveillance than is browsing activity on the average laptop.[3]

Many public libraries see the need to respond to these concerns by standing up firmly in defense of what the United Nations has called the basic human right to privacy,[4] seeking both to ensure their patrons access to privacy within the library, and to educate their communities about external threats that jeopardize the public. The currently dismal state of privacy should be of particular concern to libraries, as privacy has been one of the core values of the American Library Association (ALA) since 1939 and is part of its Bill of Rights.[5] Librarians have fought

---

[1] Mary Madden and Lee Rainie. "Americans' Attitudes about Privacy, Security, and Surveillance," accessed June 3, 2017, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/. (Pew Research Center, May 2015).

[2] Amanda Hess, "How Privacy Became a Commodity for the Rich and Powerful," accessed June 5, 2017, https://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html.

[3] Jordan Pearson, "Digital Surveillance is Class Warfare," accessed June 5, 2017, https://motherboard.vice.com/en_us/article/digital-surveillance-is-class-warfare.

[4] United Nations General Assembly. Article 12, "Universal Declaration of Human Rights." General Assembly Resolution 217 A. Paris, France. December 10, 1948; Toby Mendel et al. *Global Survey on Internet Privacy and Freedom of Expression.* (Paris: UNESCO, 2012), 11; Leslie Harris et al. "Promoting Freedom of Expression and Privacy Online," Discussion panel at Multistakeholder First WSIS+10 Review Event, UNESCO Headquarters, Paris, February 26, 2013.

[5]American Library Association. "Privacy: An Interpretation of the Library Bill of Rights," accessed June 2, 2017, http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.

vociferously against privacy violations at least since the McCarthy Era, and ALA continues to make privacy a priority through initiatives like "Choose Privacy Week" (https://chooseprivacyweek.org/).

This project will build upon the professional values set forth by ALA, going further to give librarians the practical, 21st century skills they need to safeguard patron privacy in the digital era. Library Freedom Project, a nonprofit organization fiscally sponsored by The Tor Project, Inc., has been leading this work in libraries for several years. LFP's highly successful privacy workshop program has trained an average of 1,500 librarians per year since 2013. LFP's workshops range from basic one-hour webinars that help librarians get acquainted with the landscape of digital privacy, to professional development workshops that span several days and tackle practical privacy problems in depth, exposing learners to contemporary privacy tools in a hands-on environment (see instructional slides for an "All About Tor for Libraries" workshop, appended to our sample curriculum attachment). LFP brings experts in the field from the American Civil Liberties Union (ACLU), Electronic Frontier Foundation (EFF), and other organizations dedicated to civil liberties or privacy technologies. LFP has conducted these trainings across the United States, Canada, England, Scotland, and Ireland, and has received accolades from the library world and across the privacy field. In 2015, LFP's director, Alison Macrina, was named a *Library Journal* "Mover and Shaker," and in 2016, LFP won the Free Software Foundation's prestigious Award for Projects of Social Benefit. In addition, *The Daily Dot* named Macrina one of its "Heroes Who Saved the Internet in 2015," and the New York Library Association awarded Library Freedom Project its annual Intellectual Freedom Award. LFP's work has been profiled in media publications like *The Nation*, *ProPublica*, *Motherboard*, *On the Media*, and *All Things Considered*.

After four years of privacy leadership in the library world, LFP is prepared to meet the challenge of moving from conducting workshops to the more extensive training of library-based Privacy Advocates. By collaborating with NYU educators, who bring decades of experience in building curriculum for emerging subject areas, LFP can move from workshop-based training to more intensive professional development, enabling librarians to bring effective privacy practice and education to their own institutions and communities.

Working together, NYU and LFP will build on the latter's workshops to create the Library Freedom Institute (LFI), an intensive six-month program that will train librarians to take on leadership roles throughout the country. LFI will give participants the necessary skills to conduct their own privacy workshops, aimed both at developing more privacy-focused library practices, and at educating community members about privacy threats and steps they can take to mitigate them. LFI will support librarians as they take a deep dive into some of the most important issues of our day, giving them an opportunity to work with experts in the field of privacy and surveillance, and helping them become expert trainers in their own right. This train-the-trainer model will strengthen the librarian profession while creating a network of local community resources to help members of the public mobilize against privacy threats.

NYU is the right partner for LFP. Professor Howard Besser has 30 years of experience creating extensive sets of curriculum in newly emerging subject areas, requiring both drawing upon disparate resources from other fields, and creating brand new curriculum. He has employed this curriculum to help create a cadre of new professionals. He has done this for digital imaging, digital preservation, and media preservation when each of these fields was new and lacked professional training. The Library Freedom Institute will build most directly on LFP's training workshops and Besser's curriculum design for the Society of American Archivists' Digital Archives Specialist (DAS) program. Similar to the DAS program, LFI will train working professionals to be well-versed in a subfield of emerging importance.

There is a significant library and public audience wanting this type of education. A 2015 Pew research report showed that the public wants libraries to provide digital education, and named privacy/security courses in particular.[6] After praising our draft proposal, Justin Hoenke, Executive Director of the Benson Memorial Library in rural Titusville, Pennsylvania (and another *Library Journal* "Mover and Shaker") writes, "I would gladly encourage

[6] John Horrigan et al. "Libraries at the Crossroads," Pew Research Center, September 2015, accessed June 2, 2017, http://www.pewinternet.org/2015/09/15/libraries-at-the-crossroads/.

one of my staff to commit a small portion of their time to this opportunity." Jamie LaRue, Director of ALA's Office of Intellectual Freedom (OIF), called our proposed Library Freedom Institute "complementary" to OIF's efforts. Scott Bonner, Director of the Ferguson Municipal Public Library District in Missouri, writes that "five hours a week for a few months is a relatively small cost for expertise that can create great and lasting change." Gretchen Caserotti, Director of Meridian Public Library in Idaho, said Library Freedom Institute would be incredibly valuable "not just to my own library, but all public libraries."[7] That we have received such strong support for this project from librarians across the country—including a town in Western Pennsylvania affected by the absence of its former steel and lumber industries (Titusville, PA), the St. Louis suburb that catalyzed the international Black Lives Matter movement (Ferguson, MO), and the second-largest and fastest growing city in Idaho (Meridian, ID)—is testament to the diversity of communities that this work would impact.

Our project will complement and enhance similar work in the field. The Data Privacy Project, based out of New York City, gives practical privacy training to librarians in the five boroughs, but is not positioned to meet the needs of librarians elsewhere. Tactical Technology Collective is a group dedicated to making security information available and usable for many members of the public, yet they primarily work with activists and NGOs in Europe, the Middle East, and North Africa. Cryptoparties are engaging, community-centered events where people teach each other practical privacy skills, but they are mostly ad-hoc meetings, and generally concentrated in big cities where cybersecurity experts are abundant. Library Freedom Institute would be the only intensive training for librarians across the United States, focused on confronting privacy violations that are most meaningful to local communities, and grounded in the current literature and practice of librarianship.

Privacy is a major topic in current library discourse. In publications and on his blog, influential library E-Book specialist Eric Hellman has urged librarians to start paying more attention to digital security, writing in *American Libraries Magazine* that "once [librarians consider] all the threat models associated with the digital environment...practices will certainly change."[8] Barbara Fister, of *Inside Higher Ed*, has lamented that despite our history of being vocal privacy champions, "libraries are terrible at privacy," using invasive tracking technologies like Google Analytics, and feeding sensitive patron information direct to Facebook through social media buttons.[9]

In addition, a survey in the May/June 2016 edition of *Library Technology Reports* found that only about 15% of academic and large public libraries had implemented even the most basic privacy protection for web queries (HTTPS). Gary Price devotes much of his *Library Journal* INFOdocket columns to the further erosion of digital privacy. Ian Clark, in *The Journal of Radical Librarianship*, found that the new digital divide could be summarized as those with access to privacy resources, and those without—and those without are the very same marginalized people already at greatest risk. Safiya Noble has written extensively about an algorithmic bias against people of color, and has urged library and information professionals to adopt a social justice framework towards technology. LFP's founder and Director, Alison Macrina, has herself contributed to the current discourse, authoring pieces on practical library privacy for *Reference and User Services Quarterly*, *American Libraries*, and *Library Journal*. LFP has also helped bring expertise from outside the library profession into the conversation about privacy in libraries, influencing the ACLU and EFF to write pieces for librarians on responding to government information requests, implementing HTTPS, and drafting more effective privacy policies.[10]

---

[7] Letters from Hoenke, Bonner, Caserotti, and others are included in our first supporting document.
[8] Eric Hellman, "Toward the Post-Privacy Library?" accessed June 5, 2017, https://americanlibrariesmagazine.org/2015/06/16/toward-the-post-privacy-library/.
[9] Barbara Fister "Not In the Clear: Libraries and Privacy," *Inside Higher Ed*, February 12, 2015, accessed June 5, 2017, https://www.insidehighered.com/blogs/library-babel-fish/not-clear-libraries-and-privacy.
[10] Kade Crockford, "Safeguarding Intellectual Freedom: Rights and Responsibilities of Librarians in Massachusetts," accessed June 3, 2017, https://privacysos.org/libraries/; Jacob Hoffman-Andrews, "What Every Librarian Should Know About HTTPS," accessed June 3, 2017, https://www.eff.org/deeplinks/2015/05/what-every-librarian-needs-know-about-https; Gennie Gebhart and Kerry Sheehan, "Librarians, Act Now to Protect Your Users (Before

2. Project Design

To meet the increased demand for privacy training in public libraries, we will augment LFP's highly successful in-person workshops with NYU's experience in curriculum development and delivery. The resulting Library Freedom Institute will offer librarians the extensive training needed to serve as privacy workshop leaders in their own right, setting a nationwide standard for professional privacy literacy and programmatic privacy offerings in libraries. We will focus on training future trainers to create an impact-multiplier effect, working across regions, with statewide and metropolitan library organizations, and with LFP's own collaborative partners. By combining the NYU Project Director's extensive experience with merging multiple instructional delivery channels (e.g., asynchronous and synchronous webinars, blogs, self-paced instruction, group exercises, one-on-one meetings with the instructor) with the subject-matter expertise and workshop delivery experience of LFP, we will create a high profile and effective new resource for librarians and their patrons.

The Library Freedom Institute will create a network of advanced librarian-trainers, called Privacy Advocates, to serve as community anchors who deploy privacy education and infrastructure systematically. Privacy Advocates will commit to a six-month course consisting of approximately five hours of weekly instruction, readings, assignments, and other coursework, which would cover in-depth privacy issues, privacy education, and technologies. In our application invitation, we will require that applicants possess the essential technical competencies necessary for contemporary library work. Each prospective LFI student will also have to submit a letter from their library director approving the designation of five hours per week towards participation in the six-month long Library Freedom Institute. We will begin the Institute with a pilot group of ten Privacy Advocates using real-time, two-way webinars, discussion forums, blogs, and a mailing list for instructional delivery. Coursework will consist of weekly readings and hands-on assignments. The courses will mainly be taught by LFP's founder and Director, Alison Macrina, who will manage the instructional aspects of the project throughout the grant period. Expert guest lecturers from the privacy and security worlds will assist project staff in creating thorough and up-to-date lectures and materials. Coursework will be highly practical and collaborative, with group tasks like designing an online privacy class and teaching it to other Privacy Advocates, who will be encouraged to offer constructive feedback. LFP has already spent several years developing its privacy trainings for librarians based on direct feedback from workshop participants, as well as current research and best practices in the privacy field.

A typical week (see attached "Sample Weekly Curriculum Map") could feature Noah Swartz, staff technologist at the Electronic Frontier Foundation and lead developer of Privacy Badger, an extension for many web browsers that blocks invasive tracking from advertisers and other third parties. Noah and Alison would jointly conduct a lecture about third-party tracking, including how companies compete in real-time auctions for a rich set of users' browsing data, and how these companies maintain shadow profiles of Internet users. Noah and Alison would then provide examples of how such data have been misused or exploited. Privacy Advocates would download and use the Privacy Badger extension themselves, complete a series of tasks to better learn the tool, collectively discuss its applications within and outside the library, and direct follow-up questions to the instructors. An assignment for that week could be to write a lesson plan that integrates Privacy Badger and third-party tracking information into library instruction.

Privacy Advocates will also meet in person once during the six-month period for a group dinner followed by an intensive, daylong workshop in New York City. This will be an opportunity for participants to get to know each other face-to-face, hear from privacy experts in person, and potentially collaborate on a shared project, like setting up a Tor relay (i.e., a node on the Tor anonymity network that helps Internet users worldwide access the web privately). Studies of the National Digital Stewardship Residency (NDSR) program have pointed to the importance of an in-person get-together for librarians engaged in learning cutting-edge subjects.[11] We recognize that the

---

It's Too Late)," accessed June 3, 2017, https://www.eff.org/deeplinks/2016/12/librarians-act-now-protect-your-users-its-too-late.

[11] Howard Besser, "Assessment of DC National Digital Stewardship Residency Program 2014," accessed June 6 2017, http://www.digitalpreservation.gov/ndsr/documents/2014_NDSR-DC_Assessment_Report.pdf; Meridith Beck Mink, "Keepers of Our Digital Future: An Assessment of the National Digital Stewardship Residencies, 2013–

prospect of travel to New York City may seem daunting for Privacy Advocates from less accessible parts of the country, so we are committed to making LFI's in-person component manageable and affordable. Through a grant subaward, LFP would cover participant travel, lodging, ground transportation, and per diem costs. We will use NYU facilities for the group dinner and workshop to keep overall costs down. NYU's location will also give us access to many experts in the privacy field who reside in the New York City area.

At the close of the Institute, graduates will deploy their knowledge in their home libraries, with ongoing support from LFP. This support will include our continued availability over email and on live chat during monthly "office hours," future meetups for Privacy Advocates at ALA or PLA conferences, and two check-in calls after the completion of the Library Freedom Institute—one after six months, and another after one year. Privacy Advocates will also have access to LFI's resource repository and class mailing list. LFI graduates will be required to deploy some of what they learned in the course back at their home libraries by embodying the community anchor component of this project grant. We expect our Privacy Advocates to teach privacy classes to the public, train their fellow staff on privacy practices, and offer themselves as resources to other librarians in the area. Our check-in calls will monitor progress and assist with challenges.

We will conduct a pilot six-month training with just ten Privacy Advocates and use this to analyze the LFI curriculum, system of delivery, pacing, and other pedagogical aspects, revising them as needed. We will employ questionnaires, focus groups, and interviews with both participants and guest lecturers throughout the pilot period to assess the training. We have allotted the six-month pilot and an additional three months following its conclusion to undertake this evaluation and to incorporate its results into curriculum revisions for the full six-month Institute, which will be offered to 30 additional Privacy Advocates. Following administration of the full Institute, we will spend the final three months evaluating the project, revising curricular materials accordingly, and posting the revised learning resources in an online repository.

Our assessment and revisions will target many issues that go beyond the curriculum content itself. Other issues include which aspects of the curriculum are best disseminated in real-time (so that participants can ask immediate questions) or in a self-paced environment (so that participants do not have to commit to a specific instructional time period). Optimizing the use of the Institute's in-person workshop, and planning LFI instruction and assignments around participants' existing workloads are other critical issues. Instructor effectiveness, structure of assignments, curricular topics (both covered and missing), and the sequencing and pacing of sessions are still more topics that will be essential for us to examine. We will carry out assessment in these categories during the pilot phase and subsequent analysis period in order to optimize the full Library Freedom Institute for 30 participants. We will make all LFI resources publicly accessible on both LFP and NYU's websites at the conclusion of the grant period. As Project Director, Prof. Howard Besser brings extensive experience in conducting assessments and using the resulting data to revise curriculum, training, and delivery. He has done so for NYU MIAP courses over the last 14 years, for professional society workshops over decades, and for two cycles of the Library of Congress' National Digital Stewardship Residencies (NDSR-DC).

We will develop a tool to assess what each Privacy Advocate knows both at the beginning and end of the Institute. This self-assessment questionnaire (which will be similar to one that Besser developed for NDSR-DC) will allow us to measure growth in knowledge base and competencies during the Institute, and will demonstrate where the Institute was most successful, and where it might have failed. Yet the real impact of our Library Freedom Institute can only begin to be measured adequately a year or two following project completion, since the most significant impact is likely to come from changes in information user attitudes and practices that are a result of the Privacy Advocates training others. The project team is committed to continuing assessment of the impact after the IMLS funding period is completed through the gathering of metrics (such as the number of community and librarian workshops conducted by the initial set of trainees, the number of community members attending those workshops,

---

2016," Council on Library and Information Resources report 173, December 2016, accessed June 6, 2017, https://www.clir.org/pubs/reports/pub173.

and the demographics of those trained), as well as through other means**,** such as the impact on professional literature or the number and type of privacy discussions on professional conference programs. The large-scale, cultural impact that train-the-trainer programs such as these aim for—such as changes to the operation of an institution, and to the attitudes and practices of community members—are most effectively assessed several years after the conclusion of the project period.

Our two-year work plan is broken into five stages: a six-month period of initial planning and curriculum development, followed by six months running a pilot Library Freedom Institute, three months of pilot evaluation and curriculum revision, the full six-month LFI, and a final three months to evaluate the full Institute.

- **Planning: December 2017 through May 2018**
  We will begin our initial planning stage by mapping learning outcomes for our Privacy Advocates, and will use those to design the pilot curriculum. We will draw on the expertise of our advisory board and other experts in libraries and the privacy field to help design this initial curriculum.[12] We will then recruit experts in the privacy field to serve as co-trainer consultants, providing input on curriculum development and/or lectures during the Library Freedom Institute itself. We are confident that we will be successful in cultivating a fruitful roster of co-trainer consultants. LFP has a wide network of advocates, developers, and attorneys, and we have already received verbal commitments from colleagues at the EFF, ACLU, and Tor Project. During this period we will also create our course application materials and develop our assessment tools (see "Analysis and Revision" section below) and present those to NYU's Institutional Review Board for approval. We will also begin marketing the program to libraries through contact with library professional organizations, our speaking engagements, various listservs and blogs, and our presence at library conferences. In this way, we will use much of the planning period to create "buzz" and secure as many applications for the pilot Institute as possible. Later, we will finalize details related to LFI administration, such as setting up the course infrastructure and communication channels, developing workflows for putting course materials online and editing them, and dividing the course into weekly segments. Finally, we will narrow our applicants down to a diverse set of prospective students and set up interviews, and then contact our successful applicants with their initial course materials.

- **Pilot: June 2018 through November 2018**
  In our pilot phase of Library Freedom Institute, we will run the program with an initial group of ten Privacy Advocates. These Privacy Advocates will be required to complete approximately five hours of coursework per week (about one hour fixed time and the rest of it self-paced), including assignments, and we will expect and encourage collaborative work. This coursework will include objectives such as learning some of the history and design of the Internet in order to understand how Internet infrastructure has allowed for both intended and unintended privacy and security violations, reading case studies of people who have experienced serious privacy violations and connecting those stories to the possible experiences and needs of patrons in our library communities, and downloading and testing leading industry privacy tools, understanding the problems they intend to solve, and determining how to incorporate them into library instruction. As professional librarians, we expect that our Privacy Advocates will come into the program as highly competent computer users; at the close of Library Freedom Institute, they will have developed further skills as privacy experts who are capable of using, maintaining, and troubleshooting privacy technology, and will be ready to teach this material to their communities.

- **Analysis and Revision: December 2018 through February 2019**
  Our first analysis and revision period will draw on the experiences of Privacy Advocates in our pilot program in order to revise and refine the curriculum for the full Library Freedom Institute. We will administer a set of in-depth participant surveys at several points during the Institute to evaluate their experience of the course content, delivery methods, guest lecturers, assignments, and collaborative work.

[12] Please see below (p. 10) for a list of advisory board members for this project.

We will ask them to assess how the course prepared them for the outcomes we identified, namely, how effective the course was in preparing them to use, teach, advocate for, and deploy privacy practices and technologies within their library and among other librarians in their region. We will conduct a real-time remote focus group at the end of the Institute designed to supplement the quantitative data gathered with more nuanced answers that both encourage them to expand on each other's comments, and allow for a better discussion of how content composition or delivery might be improved. We will also ask our advisory board to give us critical feedback on course content and student work. Lastly, we will ask our guest lecturers to evaluate their experience participating in the course, both through a questionnaire and through interviews. We will use all of this assessment material to analyze and revise our course curriculum, delivery, assignments, instructors, etc. We will carefully plan how to implement the revised changes before the full round of the much larger Library Freedom Institute. During this period, we will also recruit and select the 30 Privacy Advocates for the full Institute.

- **Full Institute: March 2019 through August 2019**
  The full round of Library Freedom Institute will reflect the feedback we receive during the analysis and revision period in order to create an even more robust and effective curriculum for 30 Privacy Advocates. Our framework of five hours of coursework per week will likely remain, as will our general goals and outcomes for the program, but the content, guest lecturers, and assignments are subject to revision based on the earlier feedback. The revised curriculum and course content will then be posted to Library Freedom Project's LFP and NYU websites in order to make this material accessible to the entire field of librarianship.

- **Final Evaluation: September 2019 through November 2019**
  The same set of evaluation instruments that were used for the pilot period will be used for the full Institute (see "Analysis and Revision" section above). We will also ask all members of our advisory board to engage in a final examination and discussion of the curriculum, and we will incorporate their changes. Because we will not be teaching an Institute again during the grant period, our revisions will focus on the learning resources themselves, along with recommendations as to how these might best be delivered. We will post final versions of these resources on both project partner websites and on GitHub. We will use our pre- and post-tests regarding knowledge base and competencies to assess the success of the project during the grant period.

Ultimately, however, we will define the success of Library Freedom Institute by the work that our Privacy Advocates engage in after the program is over, and by the open-source curriculum we will share on Library Freedom Project's website for even more librarians who want to bring practical privacy into their libraries. We will provide continued support for our participants with monthly "office hours" and check-in calls, and will maintain the class mailing list to keep participants in contact with each other. We expect that all of our Privacy Advocates will promptly begin implementing their new skills at their home libraries.

Our goals for Library Freedom Project include both the immediate goals in the project plan and long-term goals for field-wide library impact. During the project plan, our goals are as follows:

- Run Library Freedom Institute twice, first as a pilot, then as a full program with a revised curriculum and three times as many Privacy Advocates.

- Turn that course curriculum into a robust repository of privacy resources and training strategies for librarians that is fully shareable and replicable.

- Build on the strong community ties that librarians already have by providing them tools and training to become local experts on privacy and to act as community anchors.

- Connect librarians to a network of experts in the privacy field and build relationships for advice and ongoing support.

- Create a set of 40 Privacy Advocates trained to bring high quality privacy education and practices into libraries across the country.

Because of our train-the-trainer focus, the real impact of our project will come several years down the road. We hope to redefine libraries as the standard-bearers of privacy education and resources in their local communities, and for that to happen, our Privacy Advocates must share what they know. In three years, we expect to see multiple descendants of the Library Freedom Institute blossoming in libraries across the nation, led by librarians who have gained their skills either second or third hand from our original set of 40 Privacy Advocates.

3. Diversity Plan

We will specifically seek out a diverse group of librarians to train, and we are most interested in training librarians who work in marginalized communities. We believe that privacy is not merely a civil liberty, but is also an issue of economic and social justice, as evidenced by the research of Seeta Peña Gangadharan of the New America Foundation, by Kevin Lewis of UC San Diego, and by multiple scholars featured in *Feminist Surveillance Studies*,[13] among others, which show that the loss of privacy affects historically marginalized communities more deeply than it does the general population. Marginalized groups have also generally had less access to discussions and resources about preventing and mitigating privacy threats. Privacy education can empower these communities to use the Internet more freely and safely, and can reposition libraries and librarians as community anchors for privacy in the public imagination.

In order for our Privacy Advocates to serve as true community anchors, they must reflect a real diversity of experience, location, and ethnic identity. We want to be able to reach librarians, and therefore patrons, across many different walks of life and create meaningful instruction to address a range of unique service needs. To achieve these ends, we will engage with ALA affiliates and other professional organizations working on issues of diversity, including the Association for Rural and Small Libraries; ALA's Black Caucus; the Association of Bookmobile and Outreach Services; REFORMA (the ALA caucus for Spanish-speaking populations); the American Indian Library Association; the Gay, Lesbian, Bisexual, and Transgender Round Table; and the Asian Pacific-American Librarians Association. We will also engage with the Social Responsibilities Round Table, the ALA roundtable devoted to issues of economic and racial justice, as well as ALA's Spectrum Scholarship program, which provides scholarships to people of color in order to assist them with obtaining leadership positions in the library field. In addition, we will ask our advisory board members with deep ties in communities of color, religious minorities, and rural libraries, to help us recruit a diverse set of Privacy Advocates.

In particular, we aim to recruit participants from libraries representing Muslim communities, Black communities, immigrant communities, queer and transgender communities, and economically disadvantaged communities, given the negative experiences members of these communities have often had with surveillance and encroachments on privacy. Our curriculum will also address the unique service needs of these communities. For example, queer and transgender people often experience surveillance from online "trolls" who try to uncover their sensitive personal information, and then publish it on the Internet in order to intimidate and threaten members of those communities. Many immigrants who are facing action from immigration authorities need safe ways to communicate with families, advocacy organizations, and legal assistance. People from economically disadvantaged communities generally have no personal laptop or desktop computer access, and have limited data plans on their mobile devices, so a mobile-first, low bandwidth strategy is essential to meet their needs. Our curriculum will prioritize the needs of these vulnerable communities, and we will work with experts in the privacy field, as well as our advisory board, to make sure we have addressed all of those needs.

[13] Rachel E. Dubrofsky and Shoshana Amielle Magnet, eds., *Feminist Surveillance Studies* (Durham, NC: Duke University Press, 2015).

4. National Impact

Our project supports many aspects of the "Community Anchors" IMLS project category:

- **Developing new programs that support and engage communities**
  Our project is fundamentally about participatory privacy education and systemic privacy changes in libraries, and addresses a demonstrated need in our local communities. It relies on the existing infrastructure of libraries, preparing librarians to offer local workshops for patrons, to introduce free and open source software (FOSS) that enhances privacy, and to revise internal policies and procedures to more thoroughly support the ALA's commitment to patron privacy.

- **Partnerships and educational opportunities informed by other sectors and disciplines**
  Collaborative partnerships are essential to this project. The ACLU currently joins LFP for privacy trainings, helping librarians understand their responsibilities regarding patron privacy, and has helped craft strong library privacy policies. LFP's existing relationship with technologists at The Tor Project helps it stay abreast of changing privacy technologies and deploy appropriate privacy infrastructure in libraries. LFP additionally maintains connections with activists, lawyers, and technologists at a wide array of privacy focused organizations, such as Open Whisper Systems, Privacy International, Cryptoparty Harlem, the Lucy Parsons Project, Mozilla, EFF, and more. The project team has already received commitments from some of these colleagues to collaborate on the Library Freedom Institute. We will also leverage relationships with ALA's Intellectual Freedom Round Table and the Privacy Working Group of the Research Data Alliance to both improve our curriculum and to publicize what we have done. NYU and LFP will leverage these and other partnerships with expert organizations to bring in guest lecturers and develop training materials.

- **Investigating widespread community challenges and communicating findings**
  We are committed to open education and to creating instructional support materials that can be copied and adapted for many different kinds of training, professional development, and both self-paced and classroom education. Project Director Howard Besser has a stellar record of accomplishment in that respect: the syllabi for all classes he has taught since 1993 (the year of the first visual Web browser) are accessible online, as are most student papers written for his classes, and all curriculum modules commissioned by the NYU MIAP program. The Library Freedom Institute will make all of our materials open-source through a permissive Creative Commons license so that they can be shared and redeployed in diverse library environments. Materials will be available on both the NYU and LFP websites, and will be preserved in NYU's digital repository. We will optimize both websites for Internet search discovery, and will widely publicize their existence in professional society presentations, blogs, listservs, and through conventional library publications. Our trainings will help create a set of new practices for shifting the privacy paradigm in libraries, a base of trainer-librarians across the country conversant in privacy best practices, and an open-source curriculum that can be widely used and adapted.

The Library Freedom Institute will further support the IMLS agency-level goals of preparing the public to fully participate in their communities and global society, and of reinforcing public libraries as community anchors that enhance civic engagement, cultural opportunities, and economic vitality. Our trainings will teach librarians to lead classes that establish the library as a place where community members can learn to use the Internet with greater confidence. This expands their opportunities to learn and interact with each other, and also helps them to be more self-reliant citizens. The Internet can be a hostile place, with ever-present threats to privacy and security. By offering privacy education, libraries can help communities engage with the digital world without sacrificing safety or autonomy. The Library Freedom Institute will help libraries distinguish themselves as privacy-protective spaces in their local communities.

Both NYU and LFP project staff are experienced at sharing their research, teaching, and professional activities widely, speaking at local, regional, national, and international meetings of library associations and other groups, as

well as to the media and broader public. This type of outreach and communication is critical for making this project a success. The project's Director (Besser) and Manager (Macrina) will continue to disseminate findings from the "Privacy in Libraries" project long after the grant period ends.

Our advisory board is comprised of library community and privacy field leaders that reflect a diversity of skill sets and experiences. It includes public library directors, privacy education specialists, technology experts, and professionals with a wealth of expertise about the service needs of marginalized communities.

- **Brewster Kahle**, founder and Director of Internet Archive, is highly regarded within and beyond the library world for his work in preserving the Internet for the historical record. Brewster will bring his expertise as a nonprofit director, library technology expert, privacy advocate, and all-around internet luminary.

- **Freddy Martinez** is the director of Lucy Parsons Labs, an initiative committed to accountability and public oversight for police and local government in Chicago. He is also a security researcher and trainer focused on bringing digital security to poor and working people of color in Chicago and beyond.

- **Erinn Atwater** is a PhD candidate in computer science at the University of Waterloo, where she is a member of the Cryptography, Security and Privacy (CrySP) lab and the Centre for Applied Cryptographic Research. She is also a passionate advocate for the digital security needs of women, queer, and transgender people, and works to educate the public about privacy tools as well as improve their user experience.

- **Nasma Ahmed** is a facilitator and developer working at the intersections of technology, policy, and community organizing. A great deal of Nasma's work focuses on privacy education and advocacy for black and Muslim women and youth.

- **Laura Quilte**r, Copyright and Information Policy Librarian at UMass Amherst and Adjunct Professor at Simmons College School of Library & Information Science, offers her experience in teaching intellectual freedom and other fundamental library values to new librarians, as well as her extensive background of working on policy issues within the ALA.

- **Scott Bonner**, Director of Ferguson Municipal Public Library District, made headlines in 2014 following the police shooting of Michael Brown, when he chose to keep the library open in defiance of the local ordinance to shutter all public services in the face of growing civil unrest. Bonner embodies what libraries can stand for, and represents a community very much in need of privacy literacy.

- **Eric Hellman**, founder and President of the Free Ebook Foundation and a prolific library privacy blogger, brings years of library privacy advocacy and technical expertise. Hellman has been relentless in his demand that library vendors correct major privacy violations, and that libraries implement HTTPS as a standard for their web servers.

- **T.J. Lamanna** is a librarian at Cherry Hill Public Library in New Jersey, where he works on a variety of patron-facing privacy initiatives that he began after completing an LFP training in 2015.

Please see our first supporting document for letters of commitment from our advisory board members. We are excited about the ideas that this group will bring to our grant project and its Library Freedom Institute.

We believe that our project addresses IMLS agency-wide priorities and a demonstrated need in library communities. It is grounded in current discourse, highly practical, and would likely have a long-term impact on libraries and the local communities they serve. Librarians need enhanced knowledge and tools to support the privacy of patrons' information, and NYU working with LFP is the right partnership to deliver this information. We look forward to IMLS review and comments.

New York University Library Freedom Project: Privacy in Libraries (RE-95-17-0076)

Schedule of Completion

Planning Phase	Six months (Dec 1, 2017 - May 31, 2018)
Pilot Institute	Six months (Jun 1, 2018 - Nov 30, 2018)
Analysis & Revision	Three months (Dec 1, 2018 - Feb 28, 2019)
Full Institute	Six months (Mar 1, 2019 - Aug 31, 2019)
Final Evaluation	Three months (Sep 1, 2019 - Nov 30, 2019)

	Project Year 1											
	Dec-17	**Jan-18**	**Feb-18**	**Mar-18**	**Apr-18**	**May-18**	**Jun-18**	**Jul-18**	**Aug-18**	**Sep-18**	**Oct-18**	**Nov-18**
Planning Phase	1	2	3	4	5	6						
Pilot Institute							1	2	3	4	5	6

	Project Year 2											
	Dec-18	**Jan-19**	**Feb-19**	**Mar-19**	**Apr-19**	**May-19**	**Jun-19**	**Jul-19**	**Aug-19**	**Sep-19**	**Oct-19**	**Nov-19**
Analysis & Revision	1	2	3									
Full Institute				1	2	3	4	5	6			
Final Evaluation										1	2	3

DIGITAL PRODUCT FORM

Introduction
The Institute of Museum and Library Services (IMLS) is committed to expanding public access to federally funded digital products (i.e., digital content, resources, assets, software, and datasets). The products you create with IMLS funding require careful stewardship to protect and enhance their value, and they should be freely and readily available for use and re-use by libraries, archives, museums, and the public. However, applying these principles to the development and management of digital products can be challenging. Because technology is dynamic and because we do not want to inhibit innovation, we do not want to prescribe set standards and practices that could become quickly outdated. Instead, we ask that you answer questions that address specific aspects of creating and managing digital products. Like all components of your IMLS application, your answers will be used by IMLS staff and by expert peer reviewers to evaluate your application, and they will be important in determining whether your project will be funded.

Instructions
You must provide answers to the questions in Part I. In addition, you must also complete at least one of the subsequent sections. If you intend to create or collect digital content, resources, or assets, complete Part II. If you intend to develop software, complete Part III. If you intend to create a dataset, complete Part IV.

PART I: Intellectual Property Rights and Permissions

A.1 What will be the intellectual property status of the digital products (content, resources, assets, software, or datasets) you intend to create? Who will hold the copyright(s)? How will you explain property rights and permissions to potential users (for example, by assigning a non-restrictive license such as BSD, GNU, MIT, or Creative Commons to the product)? Explain and justify your licensing selections.

The content we are creating is instructional resources. We will issue all of our project resources under a permissive Creative Commons license, CC-BY-SA 4.0 International, with Library Freedom Project as the license holder. Librarians are generally very familiar with Creative Commons licensing, however, in order to make it abundantly clear what this license permits, we will include a small Creative Commons graphic on all of our materials, which explains in brief terms what the license means, with a link to the full license.

A.2 What ownership rights will your organization assert over the new digital products and what conditions will you impose on access and use? Explain and justify any terms of access and conditions of use and detail how you will notify potential users about relevant terms or conditions.

All of our work will be licensed under Creative Commons' CC-BY-SA 4.0 International license, meaning that the work can be shared freely as long as Library Freedom Project is attributed, and as long as any derivative work is shared with a Creative Commons license. We will notify our users by including on all work a Creative Commons graphic which explains the license and its terms. The Creative Commons logo will both be displayed on the website with links to the resources, and embedded in the resources themselves. (The audio recordings will each begin with an oral statement about the Creative Commons license.) We have opted for this permissive license because we believe that open-source licensing is strongly in line with library values of access, and we think that our work will flourish if more people are able to benefit from the resources we create for the Library Freedom Institute.

A.3 If you will create any products that may involve privacy concerns, require obtaining permissions or rights, or raise any cultural sensitivities, describe the issues and how you plan to address them.

The resources we create as part of this project will be primarily course curriculum for librarians interested in using and teaching privacy tools as part of their work in public libraries. We do not anticipate that this work will involve any privacy concerns, as we do not intend to include any material that would personally identify our students or their community members. We will employ guest lecturers during some of the classes, and will require these guest lecturers to submit in writing that we can share their work as part of the overall curriculum under a CC-BY-SA 4.0 International license. We may also request that student work be included in the final resources, and if so we will obtain informed consent in the form of written permission from those students that states that the student is comfortable sharing the material under a CC-BY-SA 4.0 International license.

Part II: Projects Creating or Collecting Digital Content, Resources, or Assets

A. Creating or Collecting New Digital Content, Resources, or Assets

A.1 Describe the digital content, resources, or assets you will create or collect, the quantities of each type, and format you will use.

We will create weekly course curriculum, for a total of twenty-six weeks in each round of Library Freedom Institute. Each week will follow a theme, and will contain readings, discussion questions, audio copies of the weekly lecture, and a weekly assignment. The readings will be shared on our website with their copyright information clearly displayed on the website and embedded within the files. The materials that we have created ourselves, including the audio lectures, discussion questions, and weekly assignments, will be shared as twenty-six modular packets on our website under our CC-BY-SA 4.0 International license. These weekly course materials will be able to be reused as resources for librarians who want to study the material on their own, or can be re-purposed as curriculum for teaching classes to the public. We may also include work created by students of the program, with their informed consent, though it is difficult to estimate the number of works that process would produce. The formats we will use include MS PowerPoint (or equivalent), audio recordings of lectures in both mp3 and BWF format, and PDF copies of course readings.

A.2 List the equipment, software, and supplies that you will use to create the content, resources, or assets, or the name of the service provider that will perform the work.

We will record our audio lectures using Audacity. We will share our materials on both the Library Freedom Project and NYU's websites, with redundant copies hosted on GitHub. We will not use a third-party service provider; project principles will perform this work themselves.

A.3 List all the digital file formats (e.g., XML, TIFF, MPEG) you plan to use, along with the relevant information about the appropriate quality standards (e.g., resolution, sampling rate, or pixel dimensions).

We intend to use PPTX or PDF for sharing course documents, and MP3 (for circulation) and BWF (for preservation) for audio files. We may also create versions of the course documents in more easily editable formats (e.g. TEX or ODP), and share those alongside the PDF or PPTX versions for those users who want to more easily remix our content.

B. Workflow and Asset Maintenance/Preservation

B.1 Describe your quality control plan (i.e., how you will monitor and evaluate your workflow and products).

The vast majority of what we create will be instructional materials created or (in the case of Co-Trainers) commissioned and curated by the project team. Each piece of material will go through an editing process. That editing process will involve not only editing for content, but also copy-editing and editing for the purpose of browser display and preservation. Before posting online, each audio lecture recording will be reviewed for signal, and a human will listen to the beginning, middle, and end to assure consistent audibility. Anything posted onto the website will be funneled through either Macrina or Besser to ensure a consistent "look and feel" to the website. The project team (including the Graduate Assistant) will carefully review all the posted resources at the end of the pilot phase, and again at the end of the full Institute. In addition, the main web page will include a link for reporting any access problems.

B.2 Describe your plan for preserving and maintaining digital assets during and after the award period of performance. Your plan may address storage systems, shared repositories, technical documentation, migration planning, and commitment of organizational funding for these purposes. Please note: You may charge the federal award before closeout for the costs of publication or sharing of research results if the costs are not incurred during the period of performance of the federal award (see 2 C.F.R. § 200.461).

Instructional material in PDF and BWF are likely to have a life well exceeding a decade. Slightly more fragile is the html used to organize this material. As an academic unit focused on digital preservation, NYU's MIAP program has a good track record of keeping similar material (both assets and the web pages providing access to them) alive and accessible; currently MIAP provides access to material since its inception 15 years ago, and plans to keep the Digital Privacy material accessible as long as MIAP exists. In addition, the materials will be deposited in the NYU Library's digital repository and in GitHub (which has a decade-long track record of keeping software accessible). At some point in the distant future when today's normal PDFs become archaic, we expect that the NYU digital repository will make a decision of which assets are important enough to migrate. (At that point, we expect that the assets will be most important for historical purposes rather than re-mixing them for then-current instructional purposes.)

C. Metadata

C.1 Describe how you will produce any and all technical, descriptive, administrative, or preservation metadata. Specify which standards you will use for the metadata structure (e.g., MARC, Dublin Core, Encoded Archival Description, PBCore, PREMIS) and metadata content (e.g., thesauri).

We do not anticipate that many people will seek to access these assets using any standard metadata scheme. (For example, Dublin Core plans for instructional material metadata never were implemented.) In general, those seeking learning objects look for them via general subject area, and do not search for age groupings, type of instructional delivery, etc. We expect that most potential users of this material will either hear about the material from our writings, public speaking, PR, listservs, blogs, etc. And we will embed meta tags with "Privacy Instruction" on all our html guide pages to facilitate discovery through search engines. In addition, we will embed Learning Objects metadata (IEEE 1484.12.1) within our lead page, though we do not feel that that will help much with discovery or precision. We will also embed technical metadata within all of our assets, and each asset entering NYU's digital repository will be assigned PREMIS metadata.

C.2 Explain your strategy for preserving and maintaining metadata created or collected during and after the award period of performance.

The only metadata collected is technical metadata which will remain embedded within the digital assets. These will survive any standard migration. The only metadata created will be meta tags within the lead pages, and these will remain embeded within those files (though their utility might change over decades). In addition, late in the project period all assets will be ingested into the NYU digital repository, and standard PREMIS metadata will be created then, and managed within the repository.

C.3 Explain what metadata sharing and/or other strategies you will use to facilitate widespread discovery and use of the digital content, resources, or assets created during your project (e.g., an API [Application Programming Interface], contributions to a digital platform, or other ways you might enable batch queries and retrieval of metadata).

We are creating a distinct type of digital resource: instructional material in the form of lectures, exercises, thought questions, etc. Discovery of one of these assets is not very useful without the context of that particular sub-topic. The lowest level of granularity for discovery will likely be the weekly sub-topic. Each weekly sub-topic will have an organizing page, complete with text description, instructional objectives, embedded meta tags, and links to each resource. It is these weekly sub-topic pages (as well as the main project page) that we want to be as discoverable as possible. We will continuously monitor and tweak these lead pages so that they are more discoverable on web search engines. And we will engage in extensive PR both to make people aware of the material on the website, and to encourage linking to it (which will enhance discoverability by search engines).

D. Access and Use

D.1 Describe how you will make the digital content, resources, or assets available to the public. Include details such as the delivery strategy (e.g., openly available online, available to specified audiences) and underlying hardware/software platforms and infrastructure (e.g., specific digital repository software or leased services, accessibility via standard web browsers, requirements for special software tools in order to use the content).

We will make all resources available without restrictions on both the LFP and NYU websites. This (and links to it) will be the primary means of access. We will also link to a GitHub repository of the same materials. GitHub is an interesting tool for dissemination because of how it handles versioning. It can be used to update and maintain the resources through community participation, while still allowing for quality control by the administrator. Accessing, downloading, and using the materials will not require any special software, just a standard web browser. Remixing the resources on GitHub will require users to install Git, either in the desktop GUI or in the command line.

D.2 Provide the name(s) and URL(s) (Uniform Resource Locator) for any examples of previous digital content, resources, or assets your organization has created.

MIAP curriculum and syllabi since 2003: http://tisch.nyu.edu/cinema-studies/miap/curriculum. Library Freedom Project's resources on using and teaching privacy tools: https://libraryfreedomproject.org/resources/. MIAP student work since 2003: http://tisch.nyu.edu/cinema-studies/miap/student-work. Course resources for one of Besser's courses dating back to 1993: http://besser.tsoa.nyu.edu/impact/.

Part III. Projects Developing Software

A. General Information

A.1 Describe the software you intend to create, including a summary of the major functions it will perform and the intended primary audience(s) it will serve.

n/a

A.2 List other existing software that wholly or partially performs the same functions, and explain how the software you intend to create is different, and justify why those differences are significant and necessary.

n/a

B. Technical Information

B.1 List the programming languages, platforms, software, or other applications you will use to create your software and explain why you chose them.

n/a

B.2 Describe how the software you intend to create will extend or interoperate with relevant existing software.

n/a

B.3 Describe any underlying additional software or system dependencies necessary to run the software you intend to create.

n/a

B.4 Describe the processes you will use for development, documentation, and for maintaining and updating documentation for users of the software.

n/a

B.5 Provide the name(s) and URL(s) for examples of any previous software your organization has created.

n/a

C. Access and Use

C.1 We expect applicants seeking federal funds for software to develop and release these products under open-source licenses to maximize access and promote reuse. What ownership rights will your organization assert over the software you intend to create, and what conditions will you impose on its access and use? Identify and explain the license under which you will release source code for the software you develop (e.g., BSD, GNU, or MIT software licenses). Explain and justify any prohibitive terms or conditions of use or access and detail how you will notify potential users about relevant terms and conditions.

n/a

C.2 Describe how you will make the software and source code available to the public and/or its intended users.

n/a

C.3 Identify where you will deposit the source code for the software you intend to develop:

Name of publicly accessible source code repository: n/a

URL: n/a

Part IV: Projects Creating Datasets

A.1 Identify the type of data you plan to collect or generate, and the purpose or intended use to which you expect it to be put. Describe the method(s) you will use and the approximate dates or intervals at which you will collect or generate it.

The only datasets we create will be from the various levels of the assessment. These will be collected at the beginning, middle, and end of both the pilot period and the full Institute. These will be used to evaluate and improve the curriculum. We do not expect re-use of this data for other purposes, and are concerned that if we preserve anything but aggregate data beyond the grant period, subsequent use of that data might lead to privacy intrusions.

A.2 Does the proposed data collection or research activity require approval by any internal review panel or institutional review board (IRB)? If so, has the proposed research activity been approved? If not, what is your plan for securing approval?

The assessment pieces will need approval from NYU's IRB. Pilot assessment plan will be submitted to the IRB in February 2018. Full Institute assessment plan will be submitted to the IRB in January 2019. Project Director Howard Besser has extensive experience at submitting this type of assessment to IRB for approval.

A.3 Will you collect any personally identifiable information (PII), confidential information (e.g., trade secrets), or proprietary information? If so, detail the specific steps you will take to protect such information while you prepare the data files for public release (e.g., data anonymization, data suppression PII, or synthetic data).

Individual data gathered will only be seen by the Project Director and Graduate Assistant (who will have gone through IRB's human subjects research training). All PII will be stripped from the dataset. Additionally, because of the small sample size in the Pilot, all data gathered will be destroyed after analysis, and only aggregate summary data will be maintained.

A.4 If you will collect additional documentation, such as consent agreements, along with the data, describe plans for preserving the documentation and ensuring that its relationship to the collected data is maintained.

Because this project is about privacy, we have a higher standard than IRB as far as protecting PII. Even if we are granted exemptions, we will still obtain consent agreements. But at the end of the each of the two evaluation periods, we will destroy both the original collected data and the consent agreements (because the small sample size could lead to identification of individuals), only keeping aggregate data. Aggregate data will be published, along with our collection instruments (original questionnaires, focus group and interview questions, etc.).

A.5 What methods will you use to collect or generate the data? Provide details about any technical requirements or dependencies that would be necessary for understanding, retrieving, displaying, or processing the dataset(s).

Collection instruments include quantitative approaches through questionnaires, and qualitative approaches through focus groups and interviews. The data will be analyzed using standard analysis instruments. The data is being used solely to inform curricular revisions, and we do not expect further use beyond that.

A.6 What documentation (e.g., data documentation, codebooks) will you capture or create along with the dataset(s)? Where will the documentation be stored and in what format(s)? How will you permanently associate and manage the documentation with the dataset(s) it describes?

Assessment data is only for internal use during the project period.

A.7 What is your plan for archiving, managing, and disseminating data after the completion of the award-funded project?

Summary aggregate data will be published, along with original questionnaires and qualitative questions asked. These will be published on our website along with the curricular materials, and the preservation plan for them is similar to that of the curricular materials (see part II above). In addition, we expect to publish articles about the assessment in traditional library journals, and some of those articles will also include questions asked and summary data. The sole use of the data gathered is to improve curriculum. We do not believe that the data will be useful for other purposes, and are afraid that making it available could lead to privacy intrusions.

A.8 Identify where you will deposit the dataset(s):

Name of repository: n/a

URL: n/a

A.9 When and how frequently will you review this data management plan? How will the implementation be monitored?

n/a