

New York University & Library Freedom Project: (More) Privacy in Libraries (RE-246272-OLS)

Statement of Broad Need:

In the two years since New York University (NYU) and Library Freedom Project (LFP) submitted our original IMLS proposal to create Library Freedom Institute, privacy has continued to be a critical topic in libraries and society at large. Some of the biggest news stories in the last two years have revealed privacy concerns in the modern world -- from the Cambridge Analytica scandal, to the passage of the EU's General Data Protection Regulation (GDPR), to the use of tools like Clearview AI with no oversight or accountability. In libraries, big vendors have made serious privacy blunders, resulting in cancelled contracts and distrust. The current crisis created by the novel coronavirus pandemic has created new privacy concerns as workplaces and universities rush to move their operations online. Despite insistence that "privacy is dead" (usually by someone whose paycheck depends on that being true), members of the public are growing increasingly concerned by this new "normal", but have nowhere to turn to learn about how to protect themselves and their communities. Librarians already occupy the position of trust in their communities that's required to provide this kind of service. Libraries serve as technology hubs, especially in communities where home internet access or desktop computers are not as easily attainable. And libraries have long considered privacy among our most sacred core values. What librarians lack are the skills required to bring accessible, community-focused privacy training to their own libraries and to their constituent communities. That's why we created Library Freedom Institute.

Library Freedom Institute (LFI) is an entirely unique professional development program to turn librarians into Privacy Advocates. It has thus far focused on intensive training (4-6 months, 5 hours/week) in both technology and policy. And pedagogically it has focused on a cohort model, where trainees work on projects together and learn to identify as part of a supportive group working on privacy challenges with one another. One of our parent organizations, Library Freedom Project, has built a network of journalists, privacy researchers, technologists, and privacy advocacy organizations, and we leverage this network to bring our weekly expert guest lecturers to Library Freedom Institute. The combination of our collaborative cohort model and our contacts in the privacy field has enabled us to create a totally unique learning experience and community of privacy-minded librarians. Library Freedom Institute complements and incorporates the work of other library privacy advocacy efforts such as the Digital Privacy Project, the IMLS-funded Privacy Field Guides, the IMLS-funded Data Doubles Project, and more, by bringing in principals from these projects as some of our weekly expert guest lecturers. The combination of our demonstrated expertise, strong reputation in and out of the library world, rigorous and relevant curriculum, and collaborative training approach has helped our 43 Privacy Advocates from the first two LFI cohorts to thrive -- teaching classes, speaking at conferences, serving as leadership in library decision-making bodies and on ALA Committees. It's this success that's led us to the maintenance and enhancement phase of our work, where we want to continue a modified form of our professional development program for librarians while also investing in the community of librarians who have graduated from the program.

We are seeking IMLS support to enhance Library Freedom Institute and make the network of Privacy Advocates more sustainable. Significant support from IMLS helped create our current community of Privacy Advocates. The pilot program of LFI took place in 2018, we have been successfully scaling the project with our first full cohort completed in 2019, and our third cohort

New York University & Library Freedom Project: (More) Privacy in Libraries (RE-246272-OLS)

beginning as of the writing of this proposal. Based on these experiences and data from our participant evaluations¹, we know that the next phase for Library Freedom Institute is to take care of and invest in what we've built by running an annual conference for all graduates, supporting regular 1:1 and group checkin calls, and running shorter versions of our training program so that more librarians can participate and so that our Privacy Advocates can share their knowledge and investment in the community as expert guest lecturers. Our advocates are deeply committed to remaining part of this community, and by shifting our focus to enhancing their knowledge, skills, and public advocacy experience, we can ensure the sustainability of our community of Privacy Advocates into the future.

Project Design:

Library Freedom Institute is designed to be accessible, relevant, and practical to the needs of professional librarians who want to offer high-quality privacy training to their communities. We use a collaborative cohort model where participants can learn from and support each other, while engaging in a rigorous curriculum including interactive guest lectures from privacy experts both inside and outside the library field. We are proposing to enhance this current model by offering shorter, focused cohorts that we think will be more accessible to busy professional librarians. We're also proposing several strategies to aid in the continued engagement of our existing Privacy Advocates through regular checkins, an annual conference, and appearing as guest lecturers in our shorter future cohorts. .

In order to better understand our project design and its rationale, some background on the history of Library Freedom Institute is necessary. LFI was born from Library Freedom Project (LFP), an initiative started by Alison Macrina in 2015. The mission of Library Freedom Project is to make real the promise of intellectual freedom in libraries by teaching librarians and their local communities about privacy threats, privacy rights, and anti-surveillance strategies that can be used by people across technical skill levels. Library Freedom Project has been recognized nationally and internationally for our work in the field, including founder Alison Macrina being named one of *Library Journal's* "Movers and Shakers" in 2015. After two successful years teaching hundreds of librarians how to defend privacy, Alison decided to scale LFP's shorter trainings into an intensive program for dedicated librarians, and thanks to our first IMLS grant, Library Freedom Institute was born. LFP teamed up with Dr. Howard Besser at New York University (NYU) for assistance with pedagogical strategies and curriculum design, and Howard and Alison worked together to create a high-quality training program that addresses the demand for privacy literacy in libraries.

Besser (an Emeritus Professor of Library Science and Founding Director of a quasi-MLIS degree at NYU) has more than 15 years of experience using group exercises within a cohort model to create groups of graduates who continued to collaborate with each other for decades beyond their graduation. His program had great success in creating leaders dedicated to advancing the field and teaching workshops designed to provide lifelong learning opportunities for others in the field. And his graduates are widely known for their active engagement with community groups (particularly

¹ Supporting documents, including participant evaluations from 2019, are here <https://tinyurl.com/lfi2020>

New York University & Library Freedom Project: (More) Privacy in Libraries (RE-246272-OLS)

disempowered ones). And Besser has more than 30 years of experience giving his students practical assignments designed to be useful for other professionals in the field (and has been posting these works online since 1993).

In the first three years of Library Freedom Institute, participants have learned about privacy issues over a four to six month period, through a combination of weekly lectures from experts in the privacy field, an online discussion forum, group projects, and readings². Our rigorous and relevant curriculum covers a huge amount of ground in the privacy world. We discuss how to evaluate vendor policies for privacy, and how to demand better practices in our contracts with them. We talk about using privacy tools on public computer environments, and teaching privacy-focused computer classes appropriate for various needs and digital literacy levels. We discuss privacy issues out in the world -- from data brokers and “doxing” (the practice of nonconsensually collecting and sharing personal information in order to harm someone), to the data collection practices of large companies like Facebook and Google. We discuss privacy rights and how to exercise them in the networked world. In all of our topics, we make sure the information is fresh and relevant, and includes ways to employ the information or practice in a variety of library settings.

Cohort participants have then worked together through ongoing experimentation with programming and library policies - as well as final group projects - to formulate practices and create deliverables to help develop a privacy-centric culture. These materials can be used in their home libraries and have been made available through LFP’s website to any librarian who wants to bring privacy into their library.

Upon completing Library Freedom Institute, the cohort participants became Privacy Advocates within the Library Freedom Project, and the work is far from over. We’ve created a true community of practice where our Privacy Advocates continue to work together to assess their privacy practices, give talks and trainings, and serve as privacy “thought leaders” in the library world. In our formal assessments of cohorts one and two, participants reported that the collaborative, community-focused aspects of LFI were what they found most valuable (and had only positive feedback about all other components of the program). Our Privacy Advocates are now empowered to serve in leadership capacities across the library world. The first 2020 cohort is just beginning as of the writing of this proposal, and we received a record number of more than 100 applicants to that cohort for only two dozen slots.

We’d like to enhance this work by:

- *Creating shorter, more topically focused cohorts, expanding this opportunity to more busy professional librarians*
- *Strengthening the community of LFI Privacy Advocates and keeping them engaged by bringing them in as expert lecturers for these shorter cohorts*
- *Hosting our first annual meeting for all LFI graduates to learn, build community, and find new opportunities for collaboration*

² Examples of curriculum, participant final projects, and other supporting documents are here: <https://tinyurl.com/lfi2020>

New York University & Library Freedom Project: (More) Privacy in Libraries (RE-246272-OLS)

- Supporting our Privacy Advocates with monthly checkins, collaborative work, and feedback from project managers in order to build longterm sustainability of the Advocates group

We have proposed the shorter cohort lengths in order to expand this opportunity to a much larger pool of applicants. We repeatedly hear from librarians who are interested in taking our training, but can't justify the 4-6 month time commitment. We decided that the best way to offer shorter cohorts without sacrificing any of the content was to offer two 2-month cohort models focused on distinct subject areas: one about programming, training, and outreach, and the other about library systems and policies. We used the survey data from previous cohorts to identify these two subject categories as the most relevant and engaging. Those survey results also demonstrated the continued need for monthly cohort calls and quarterly 1:1 meetings with Alison Macrina, which is our justification for her increased time on activities other than direct instruction. Our advocates said that this regular group and individual checkin time is vital for feeling a continued sense of community and for helping develop collaborative conference proposals and projects. Finally, a combination of the survey data and individual conversations with our advocates confirmed that they were very interested in roles as expert guest lecturers for the future cohorts. Our advocates are proud of the work they're doing and are eager to share that and what they've learned with the next wave of Privacy Advocates.

Our 2+ year work plan will consist of four two-month Institutes with focused curricula and a three-day meeting for our graduates. We'll also provide year-round support for our Privacy Advocates during the planning and evaluation phases via monthly calls, quarterly 1:1 meetings, and ongoing asynchronous communication on our discussion forum. Our 2+ year work plan outline is as follows.

- Planning stage (6 mos): Coordinating with Privacy Advocates, creating curriculum, and seeking diverse applicants through targeted outreach. Though our official start date is September 1, 2020, we will not be expending any funds until December 1, 2020. We will be using that time for additional planning including the incorporation of evaluation results from our previous IMLS grant, which will become available in October 2020. This planning stage includes those first three months where we will not begin using the funding yet. Because of uncertainties due to the coronavirus pandemic, we are building in extra planning time in advance of drawing down project funds. Our attached budget begins on December 1, 2020.
- First LFI (2 mos): Focused on privacy in library systems and policies, taught by project lead Alison Macrina and Privacy Advocates from former Institutes.
- Evaluation, revising, planning, and recruitment (3 mos): Evaluate the first shorter cohort and prepare for the next two-month round, focused on programming, training, and outreach.
- Second LFI (2 mos): Focused on privacy programming, training, and outreach.
- Evaluation, revising, planning, and recruitment (3 mos): Evaluate the second shorter LFI and plan our annual meeting for all LFI graduates.
- Third LFI (2 mos): Focused on systems and policies.
- Meeting planning (2 mos): Preparing and executing the first annual convening for Privacy Advocates with guest speakers and interactive programming.
- Annual Meeting: Convening Privacy Advocates for 3 days to collaborate and learn.

New York University & Library Freedom Project: (More) Privacy in Libraries (RE-246272-OLS)

- *Evaluation, revising, planning, and recruitment (3 mos)*: Meeting evaluation, prep and outreach for next LFI round.
- *Fourth LFI (2 mos)*: Focused on programming and outreach.
- *Final evaluation and wrap-up (2 mos)*

After running Library Freedom Institute for two cohorts, our biggest lesson learned is that the greatest strength of LFI is in its collaborative elements. The two cohorts that have graduated learned the most during the course by working together, and have taken that collaborative spirit to continue doing work together in their home libraries and regions (see the section “Broad Impact” and the document “Privacy Advocates post-cohort work” linked here <https://tinyurl.com/lfi2020> for more details). This work requires continual learning and a creative approach, and the LFI community supports those efforts.

That’s why sustaining and enhancing the Library Freedom community is the most important next step for this program. We’ve begun holding monthly all-cohort calls to check in on all the work that the Privacy Advocates are doing, share successes and challenges, and discuss ideas for future collaboration. Every quarter, each graduate meets with Alison Macrina to discuss their work one-on-one. Before big state-level and national conferences, we coordinate on talks and other events to make sure our advocates are working together and making time to see each other face-to-face. Our alumni network is likely without parallel in the library world, and we intend to keep the group together. We think our proposed workplan is the best way to continue supporting that community and to enhance its long-term sustainability.

Another unique aspect of Library Freedom Institute’s project design is our strategic partnerships with experts across the privacy field. These partnerships were sustained through the professional network Alison Macrina has built in five years of running Library Freedom Project, and include organizations like Electronic Frontier Foundation, Black Movement Law Project, the American Civil Liberties Union, Freedom of the Press Foundation, AI Now Institute and a number of other organizations offering legal, advocacy, and technical expertise. In the current phase of Library Freedom Institute, Alison has worked with these partners to determine the weekly class topics and themes. The organizational partners are then available to support our advocates in their future work. For example, the ACLU of Massachusetts has continued to work closely with our advocates in the state of Massachusetts and beyond on efforts to mitigate the downsides of how facial recognition is employed. Other partners have offered advice and feedback on our advocates work, and have made themselves available for in-person library programming events. The community that we’re building is not just among the graduates of our program, but with the broader privacy advocacy world. Our proposed shorter cohorts will leverage the expertise of our Privacy Advocates for our weekly lectures, but will still include support and feedback from our many strategic partnerships (and likely a lecture or two from them as well).

Our project plan includes continued evaluation to measure our success. We used in-depth surveys and interviews to modify each subsequent cohort of Library Freedom Institute curriculum to meet our pedagogical objectives and our Privacy Advocates’ needs. We conducted our surveys at the end of each cohort, and solicited individual feedback from each participant mid-way through the cohort,

New York University & Library Freedom Project: (More) Privacy in Libraries (RE-246272-OLS)

at the end, and then during our quarterly one-to-one calls. We also sought input from our board of advisors and from our expert guest lecturers. We will continue this iterative evaluation/redesign-of-curriculum process throughout the future LFI cohorts and as we design the annual meeting.

We share the results of this program in a number of ways. Our website is the most direct way to benefit from this work. We list our graduates there and have a contact form for anyone who wants to bring a Privacy Advocate to their library for a talk or training. Our graduates have created many resources available there to download, including a Guide to Protecting Yourself From Online Harassment, a Library Vendor Privacy Scorecard, a presentation on Census 2020 privacy, bookmarks with tips on protecting privacy, and more, all available at the “resources” tab on our website.³ Finally, many of the talks and curriculum from past Institutes can be found on our wiki⁴ (and linked here <https://tinyurl.com/lfi2020> under “Privacy Advocates post-cohort work”). We will continue to host all of our materials openly, using a permissive open-source license so that as many people as possible can benefit, and so that others can design workshops and curriculum based on the work that we’ve done.

The continued success of Library Freedom Institute means an even stronger community of Privacy Advocates in more libraries around the country. It means more collaboration between graduates of each cohort and across cohorts, supporting one another to take necessary pro-privacy action in their libraries. It means a greater set of librarians who can participate on a shorter timeline. And most importantly, it means that the people in our communities who are most impacted by the loss of privacy will know who they can rely on to help them navigate the complicated world of Big Data and surveillance. More Library Freedom Institute means positioning more libraries as privacy hubs.

Diversity Plan: The loss of privacy disproportionately affects marginalized groups, so diversity is paramount to this project. We have successfully incorporated diversity into this program in several ways: we aim for diverse participants, diverse lecturers, weekly topics that focus on the loss of privacy to marginalized people, and materials that address the specific concerns of those people. And we feel that we have been successful beyond our wildest dreams. For example, our first two cohorts participants have been 36% self-identified Black, Indigenous, and/or People of Color (BIPOC), and 35% are from rural or southern libraries. Our guest lecturers in the first two cohorts have been 32% BIPOC, and we are on track to exceed that number in our 2020 cohorts.

In order to reach diverse applicants, we use targeted outreach and promotion of our diverse graduates. When in our recruitment phase, we take special care to promote the program to groups focused on BIPOC in libraries, like ALA Spectrum Scholars, the Black Caucus of ALA, and REFORMA. In addition to racial and ethnic diversity, we recruit heavily among rural and southern library professional organizations, since these libraries tend to have less funding for professional development opportunities and since their communities also represent many people who are uniquely harmed by the loss of privacy. We also conduct in-person recruiting at conferences like

³ <https://libraryfreedom.org/index.php/resources/>

⁴ https://libraryfreedom.wiki/html/public_html/index.php/Main_Page/Talks_etc

New York University & Library Freedom Project: (More) Privacy in Libraries (RE-246272-OLS)

ALA and PLA with our diverse Privacy Advocates joining us to talk to prospective applicants about their experiences. This approach to recruitment has helped applicants see themselves reflected in the previous cohorts, and our success in this approach is reflected in the makeup of our cohorts. Our first cohorts were each comprised of about 36% people of color; our current cohort is 67% women, 23% men, and 10% non-binary people. We have attained geographic diversity, making sure to always have a significant number of librarians from the deep south and rural libraries. We have also prioritized public libraries and community college libraries who are less likely to have professional development funding for staff.

We have also prioritized diversity among our guest lecturers, and have focused the weekly Institute topics on surveillance and marginalized people. In the 2019 program, 40% of our guest speakers were self-identified BIPOC. Some of the topics we covered included how police target Black and Brown communities with surveillance, the racial and gender biases of facial recognition software and other artificial intelligence tools, digital discrimination against poor communities and communities of color, and making digital privacy accessible to people with disabilities, elderly people, and immigrants. In our first few weeks of the course, we discuss the concept of “threat modeling” -- which is the idea that everyone in every circumstance has a reason to need privacy -- and we discuss example threat models, like “LGBT youth” or “undocumented person”. We use this framework to guide every subsequent discussion about threats, strategies, and tools. Since we build our curriculum through continuous feedback and evaluation from our cohort participants, it also reflects their experiences and the experiences of the communities they serve.

Finally, the real measure of our diversity and inclusion efforts is in how we retain and continue to support the diverse set of Privacy Advocates we’re training. From a study he worked on 30 years ago⁵ Besser has been acutely aware that one of the biggest challenges in educating historically marginalized groups is not so much in admitting them into a program, but retaining or keeping them actively involved. This is the motivation for our entire proposal and workplan. By investing in our Privacy Advocates through regular 1:1 conversations with Alison Macrina, monthly group calls, and an annual conference, we’ll be able to provide the crucial support to keep our advocates engaged. By appearing as guest lecturers to the smaller, focused cohorts, they can feel even more invested in the project by sharing their knowledge and experience with other librarians like them. These regular engagements will also be time to develop Library Freedom’s future together. We think there’s no better way to ensure the continued participation of our diverse set of Privacy Advocates than by making the future of Library Freedom theirs to design.

Broad Impact: LFI is a nationwide project supporting the IMLS project category of “Community Catalysts”. With our graduated advocates representing 22 states and the District of Columbia, and a mix of urban, suburban, and rural libraries (and eleven in the south), our work is unique in its range. Our strategic collaborations reach across the privacy field -- partnerships with prominent organizations like the American Civil Liberties Union and Electronic Frontier Foundation, as well as privacy leaders from the library world, inform our practice and enhance our impact. The programs

⁵ Duster, T. (1991). *The diversity project: Final report*. Berkeley: Institute for the Study of Social Change. *University of California, Berkeley*.

New York University & Library Freedom Project: (More) Privacy in Libraries (RE-246272-OLS)

that our Privacy Advocates deliver in their libraries support community well-being and engagement, and are in high-demand as interest in privacy grows. Our goals to enhance LFI will continue to broaden its impact with more trained librarians in more places, and a resilient and supported community of practitioners.

The depth and breadth of the impact of this project is evident in the work our Privacy Advocates have been doing together -- offering talks and trainings in their regions, supporting privacy in their home libraries, and working collaboratively to make it all happen. Here's just a snapshot of what some of our advocates are up to:

Vendor privacy and accountability: Qiana Johnson, Northwestern University (Chicago, Illinois) and Nicole Becwar, Western University (Gunnison, Colorado). Qiana and Nicole have studied the privacy policies of dozens of library vendors as well as best practices for data protection and minimization. They then created a rubric to measure the efficacy of these policies, grading them on criteria like “can users request that their data be deleted?” and “are there options for opting in or out?”. Policies are then graded either green, yellow, or red, with further information on what these grades mean and how vendors can improve.

Privacy for domestic violence survivors, with an emphasis on Spanish speakers: Wren Kominos-Marvell, Teton County Library (Jackson, Wyoming). Working directly with the local domestic violence shelter in Jackson, Wren has created a set of resources and trainings for addressing the privacy needs of domestic violence victims. These resources are in both English and Spanish and discuss common practices used by abusers to violate the privacy of their victims. The trainings are designed to address these concerns in a safe way.

Census 2020 and privacy concerns: Jeff Lambert (Queens Public Library) and Carolyn Bennett Glauda (Southeastern New York Library Resources Council) have both worked on educating librarians in New York state (and beyond) about the upcoming 2020 Census, anticipating privacy concerns and questions from patrons and preparing librarians to navigate them.

Privacy for online learning environments: In light of the emerging public health crisis surrounding the novel coronavirus and the closures of schools and universities, our Privacy Advocates from cohorts one and two worked together swiftly on a resource to protect privacy in online learning environments⁶. Their immediate responsiveness to this growing crisis exemplifies the way these cohorts work together, their commitment to each other and to their respective communities.

Not only are our Privacy Advocates doing incredible work out in the field, but they describe their experiences with Library Freedom Project as deeply impactful for them personally. Here are a few of their testimonials:

⁶ https://libraryfreedom.wiki/html/public_html/index.php/Privacy_for_online_teaching

**New York University & Library Freedom Project: (More) Privacy in Libraries
(RE-246272-OLS)**

“The 2019 cohort of Library Freedom Institute (LFI) started at about the one year mark of career as a teen librarian. I've ended up doing work I never would have thought I was capable of, and it is all due to the program and the network of support Alison has built with Library Freedom Project.”

“The library is one of very few spaces where this conversation about privacy and surveillance is happening. It is very important that critical space be given over in libraries to have conversations about surveillance and the power that wields it, alongside workshops and other programs that engage library users in creative ways. The LFI course provided an opportunity for this cohort to explore these topics and engage other librarians who may work in other disciplines, getting a fuller perspective of the threats invasive technology poses. LFI is a vital resource for librarians who want to pick this issue up and challenge their community to demand better.”

“Participating in the Library Freedom Institute gave me the opportunity to think and learn broadly about various privacy issues. And the final project was particularly helpful in giving me the opportunity to think about privacy issues as it related to my particular area of librarianship. Since finishing LFI, I have had the opportunity to present locally and nationally about privacy issues in libraries. Finally, the cohorts have provided a community of colleagues that continue to support each other in our ongoing work of educating our communities about privacy issues as well as advocating for privacy protecting policies and practices in our communities.”

“Library Freedom Institute provided privacy education I did not receive in my MLIS program. The combination of weekly lectures, in person training, and collaborative projects created a remarkable praxis, where we were able to apply our learning and create something real and concrete. The cohort created a Data Hygiene Calendar that helps patrons maintain healthy data habits. LFI also connected me with other privacy advocates in my state and we are working on a privacy proclamation with our state library association. LFI provides the privacy praxis so desperately needed in the information professions.”

“The weekend training at NYU was the most seen, heard, and respected I have ever felt in my career. The work LFI is doing is absolutely transformational. I came back from that training with more career confidence than I've ever had. LFI not only builds better privacy advocates, but better people.”

“The institute has just been an amazing experience. One important aspect of the institute for me was that, as a librarian, I thought I knew a lot about privacy issues only to learn that I had a very basic understanding of privacy concerns that libraries and patrons are currently facing. Just this morning I laid out an agenda for myself to revisit all of the course materials/webinars to make sure I absorbed everything that I wanted to and need to. Again, I feel like I am now part of a community of privacy advocate librarians. I have a webinar that I am teaching with another cohort member in the spring. Also, I will be presenting at ALA with two other cohort members. In the fall, I did a presentation at our state conference and

New York University & Library Freedom Project: (More) Privacy in Libraries (RE-246272-OLS)

should be doing a similar one regionally this spring. All of these presentations are on privacy issues. I've also been asked to be the first chair on a privacy, security, and accessibility committee with our library consortium. All of this would not have been possible without LFI. It is truly a transformative experience.”

“As a CEO of a Library System, it is the first time that I have experienced a welcoming and engaging learning environment. Alison brought an amazing and smart group of people together, whose goal was to learn, discuss and respect each other's opinions, character and learning method. Each topic brought a hard reality to light but having meaningful conversations made it easy not to get overwhelmed. Thank you for the opportunity.”

“The most informative and rewarding professional development I've taken part in my professional career.”

“I pitch this program to everyone I know, the cohort was absolutely fantastic and a necessary step for librarians looking to make positive change in their community.”

“Every librarian or library student should take a curriculum such as LFI. It is an invaluable resource for the profession.”

“This was a life changing and eye-opening experience.”

These testimonials only begin to tell the story of what this community means to each other. Another great example of just how impactful this program has been to our Privacy Advocates came at the American Library Association’s Midwinter Meeting in Philadelphia in January⁷. Eleven of our Privacy Advocates joined us in Philly to help staff the exhibit booth and help us recruit applicants to the next Library Freedom Institute. Many of them only attended ALA for this (with the blessings of their institutions), and in spite of only scheduling three advocates at a time on the booth, almost all eleven of them could be found at the booth at any given time during the weekend. Their enthusiasm for the program was infectious, and it was incredible to see them express so much pride in their work and excitement about our community. They loved being there with each other and it showed. There was no better marketing we could have done than having this group present to share their experiences with potential applicants.

Finally, we were pleased to read the preliminary reviewer comments which recognized the impact of our work, with comments like “The strongest component to this proposal is its demonstrated understanding of the library field within a larger societal lens.”; “This project demonstrates how the cohort experience can stimulate growth in these important and urgent conversations related to privacy that can certainly influence both practice and the theory that emerges from what here can become everyday library practice.” and “This proposal represents a logical, encouraging step forward

⁷ Photos from ALA Midwinter and other LFI in-person events can be found in our appendices <https://tinyurl.com/lfi2020>

**New York University & Library Freedom Project: (More) Privacy in Libraries
(RE-246272-OLS)**

for a program that has proven itself to be a source of positive, meaningful influence. The subject matter is refreshingly current, and the approaches are innovative and exciting. Further the details in the proposal represent an iterative design process from the project team.” Other reviewers noted how much this proposal fits into the IMLS agency wide goals, saying, “The project aim to grow a community of librarians and, therefore, concerned libraries also connects to the Diversity, Equity, and Inclusion indicator in ways that re-center the Community Catalyst and an emphasis on Lifelong Learning as a circular model of collaboration in which those LFI participants leave as Privacy Advocates and, in turn, train next and future cohorts of librarians to become Privacy Advocates.”

With IMLS support for the next stage of our high-quality privacy trainings, and the ability to nurture our existing community of Privacy Advocates, there is almost no limit to the impact this project can have. We are deeply grateful for the support that IMLS has already provided us, and we are honored to be considered for this next round of funding.

New York University & Library Freedom Project: (More) Privacy in Libraries (RE-246272-OLS)

Schedule of Completion

Planning Stage	Six months (September 1, 2020 - February 28, 2021)
Training 1-LFI systems and policies	Two months (March 1, 2021 - April 30, 2021)
Evaluation-1 and revising planning, recruitment for #2	Three months (May 1, 2021 - July 31, 2021)
Training 2-LFI programming and outreach	Two months (August 1, 2021 - September 30, 2021)
Evaluation-2 and revising planning, recruitment for #3	Three months (October 1, 2021 - December 31, 2021)
Training 3-LFI systems and policies	Two months (January 1, 2022 - February 28, 2022)
Meeting planning	Two months (March 1, 2022 - April 30, 2022)
Annual meeting	Three days, taking place sometime in 2022
Evaluation-3 and revising planning, recruitment for #4	Three months (May 1, 2022 - July 31, 2022)
Training 4-LFI programming and outreach	Two months (August 1, 2022 - September 30, 2022)
Final Evaluation, summarizing and disseminating project results	Two months (October 1, 2022 - November 30, 2022)

Project Year 1												
	Sep-20	Oct-20	Nov-20	Dec-20	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21
Planning Stage	1	2	3	4	5	6						
Training 1-LFI systems and policies							1	2				
Evaluation-1 and revising planning, recruitment for #2									1	2	3	
Training 2-LFI programming and outreach												1

Project Year 2												
	Sep-21	Oct-21	Nov-21	Dec-21	Jan-22	Feb-22	Mar-22	Apr-22	May-22	Jun-22	Jul-22	Aug-22
Training 2-LFI programming and outreach	2											
Evaluation-2 and revising planning, recruitment for #3		1	2	3								
Training 3-LFI systems and policies					1	2						
Meeting planning							1	2				
Annual meeting								1*				
Evaluation-3 and revising planning, recruitment for #4									1	2	3	
Training 4-LFI programming and outreach												1

*Annual meeting date is approximate and will take place sometime in mid-2022

Project Year 3			
	Sep-22	Oct-22	Nov-22
Training 4-LFI programming and outreach	2		
Final Evaluation, summarizing and disseminating project results		1	2



DIGITAL PRODUCT FORM

INTRODUCTION

The Institute of Museum and Library Services (IMLS) is committed to expanding public access to digital products that are created using federal funds. This includes (1) digitized and born-digital content, resources, or assets; (2) software; and (3) research data (see below for more specific examples). Excluded are preliminary analyses, drafts of papers, plans for future research, peer-review assessments, and communications with colleagues.

The digital products you create with IMLS funding require effective stewardship to protect and enhance their value, and they should be freely and readily available for use and reuse by libraries, archives, museums, and the public. 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

If you propose to create digital products in the course of your IMLS-funded project, you must first provide answers to the questions in **SECTION I: INTELLECTUAL PROPERTY RIGHTS AND PERMISSIONS**. Then consider which of the following types of digital products you will create in your project, and complete each section of the form that is applicable.

SECTION II: DIGITAL CONTENT, RESOURCES, OR ASSETS

Complete this section if your project will create digital content, resources, or assets. These include both digitized and born-digital products created by individuals, project teams, or through community gatherings during your project. Examples include, but are not limited to, still images, audio files, moving images, microfilm, object inventories, object catalogs, artworks, books, posters, curricula, field books, maps, notebooks, scientific labels, metadata schema, charts, tables, drawings, workflows, and teacher toolkits. Your project may involve making these materials available through public or access-controlled websites, kiosks, or live or recorded programs.

SECTION III: SOFTWARE

Complete this section if your project will create software, including any source code, algorithms, applications, and digital tools plus the accompanying documentation created by you during your project.

SECTION IV: RESEARCH DATA

Complete this section if your project will create research data, including recorded factual information and supporting documentation, commonly accepted as relevant to validating research findings and to supporting scholarly publications.

SECTION I: INTELLECTUAL PROPERTY RIGHTS AND PERMISSIONS

A.1 We expect applicants seeking federal funds for developing or creating digital products to release these files under open-source licenses to maximize access and promote reuse. What will be the intellectual property status of the digital products (i.e., digital content, resources, or assets; software; research data) you intend to create? What ownership rights will your organization assert over the files you intend to create, and what conditions will you impose on their access and use? Who will hold the copyright(s)? Explain and justify your licensing selections. Identify and explain the license under which you will release the files (e.g., a non-restrictive license such as BSD, GNU, MIT, Creative Commons licenses; RightsStatements.org statements). 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.

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.

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.

SECTION II: 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 the format(s) you will use.

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

A.3 List all the digital file formats (e.g., XML, TIFF, MPEG, OBJ, DOC, PDF) you plan to use. If digitizing content, describe the quality standards (e.g., resolution, sampling rate, pixel dimensions) you will use for the files you will create.

Workflow and Asset Maintenance/Preservation

B.1 Describe your quality control plan. How will you monitor and evaluate your workflow and products?

B.2 Describe your plan for preserving and maintaining digital assets during and after the award period. Your plan should 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).

Metadata

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

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

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).

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, delivery enabled by IIIF specifications).

D.2. Provide the name(s) and URL(s) (Universal Resource Locator), DOI (Digital Object Identifier), or other persistent identifier for any examples of previous digital content, resources, or assets your organization has created.

SECTION III: SOFTWARE

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.

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

Technical Information

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

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

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

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

B.5 Provide the name(s), URL(s), and/or code repository locations for examples of any previous software your organization has created.

Access and Use

C.1 Describe how you will make the software and source code available to the public and/or its intended users.

C.2 Identify where you will deposit the source code for the software you intend to develop:

Name of publicly accessible source code repository:

URL:

SECTION IV: RESEARCH DATA

As part of the federal government's commitment to increase access to federally funded research data, Section IV represents the Data Management Plan (DMP) for research proposals and should reflect data management, dissemination, and preservation best practices in the applicant's area of research appropriate to the data that the project will generate.

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

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?

A.3 Will you collect any sensitive information? This may include personally identifiable information (PII), confidential information (e.g., trade secrets), or proprietary information. If so, detail the specific steps you will take to protect the information while you prepare it for public release (e.g., anonymizing individual identifiers, data aggregation). If the data will not be released publicly, explain why the data cannot be shared due to the protection of privacy, confidentiality, security, intellectual property, and other rights or requirements.

A.4 What technical (hardware and/or software) requirements or dependencies would be necessary for understanding retrieving, displaying, processing, or otherwise reusing the data?

A.5 What documentation (e.g., consent agreements, data documentation, codebooks, metadata, and analytical and procedural information) will you capture or create along with the data? Where will the documentation be stored and in what format(s)? How will you permanently associate and manage the documentation with the data it describes to enable future reuse?

A.6 What is your plan for managing, disseminating, and preserving data after the completion of the award-funded project?

A.7 Identify where you will deposit the data:

Name of repository:

URL:

A.8 When and how frequently will you review this data management plan? How will the implementation be monitored?