Securing our Public Libraries: A Forum on Privacy and Security

The School of Information Sciences at the University of Illinois Urbana-Champaign is seeking a grant in the amount of $150, 000 from National Leadership Grants for Libraries (NLG-L) to support a National Forum on privacy and security, enabling experts to collaborate with public library representatives in an exploratory study to gather, learn, and discuss what technological mechanisms are currently in place to protect the nation's public library patrons' privacy. More specifically this project will seek to identify the existence or absence of privacy protecting technologies (software and/or hardware) in public library systems of all sizes, considering the differences in comparing smaller rural vs. larger urban public library systems and what unique challenges they face. The results of this project will impact the capacity of library staff and patrons to access and engage with online content while protecting user privacy and library system integrity.

Statement of National Need: With over 9,000 public library systems in the US, the impact of public libraries is widespread (Rosa, 2019). American public libraries and the American Library Association (ALA) have a long-standing reputation of being on the forefront of protecting patrons' privacy dating back into the early 20th century when the ALA Code of Ethics was affirmed in 1939 (Gardner, 2002). Due to the digital revolution and changes in United States society, public libraries now play a critical role in offering free public internet access and have become a key source of news, social capital, and access to electronic government services and information for a significant proportion of the U.S. population (Jaeger & Fleischmann, 2007). Those who rely on these services include those who have no other means of access, such as people who need help using computers and the internet and populations of low socioeconomic status who are entrusting their privacy to the library system. Federal, state, and local government agencies also rely on public libraries to provide guidance and access to government websites, forms, and services and therefore direct citizens to their public library for help (Jaeger & Fleischmann, 2007). More recently, the ALA updated its interpretation of the Library Bill of Rights to include technological measures that can protect patron privacy; but with such a wide variety of library sizes, funding, staff training, equipment, vendors, and software installed on library systems, it is not clear if any widespread technological measures are currently in place that can adhere to the ALA guidelines. In addition, there has been a lack of focus on the discussion of technological measures that need to be in public libraries in order to protect the privacy of the patrons using the facilities and of the integrity of the library systems themselves.

Public libraries are an integral part of low-income households and are essential for under-represented individuals and families in the United States (UMD iSchool, 2020). These groups rely heavily on the services provided by libraries and are among the most frequent users; yet their right to privacy and intellectual freedom is the most at risk. In 2019, young adults, women and low-income households remained the most common groups to regularly visit libraries, averaging about 10.5 visits per person (Gallup, 2020). Studies show that families from impoverished areas fell victim to a significant number of phone and email scams, viruses, and incidents of online stalking. Families agreed that they found it difficult to protect themselves due to lack of knowledge of how to prevent this from happening and agreed that libraries are primary source of information for them (UMD iSchool, 2020). Surveys have shown that low-income households are highly concerned about information privacy, and concerns about privacy and security are among the highest for Hispanics and Black people (Madden, 2017.) 60% of low-income households are worried about the loss or theft of financial information, 48% say they are scared of becoming inadvertently involved with internet scams, and 52% say that a lack of understanding about what information is being collected, and why, is also concerning (Madden, 2017). With funded projects able to focus on researching and expanding existing privacy policies, libraries and library staff can more successfully protect patron privacy and ensure the right to intellectual freedom within these public facilities. The goals of this project are to collaborate directly with other public libraries and affiliates to gather more information about what technological measures are in place to protect information privacy. This project also intends to explore the demographics of who relies on public library services the most and how their privacy needs exceed that of the general population.

Why Public Libraries:

Public libraries have traditionally been an essential haven of resources for Americans, and evidence suggests that the well-being of communities who allocate more funds to their libraries has improved overall (ACRL). While some may believe that public library attendance is fleeting, in 2016, there were 1.3 billion visits to public libraries, with an average of about 4 million visits per day, affirming that libraries are a prominent source of equal access to information for Americans, one that works to inform users about healthcare, assist in job searches and finances, and offer a multitude of learning opportunities that significantly benefit those who utilize them (IMLS). Some of the primary services that public libraries offer are computer software training (84% of libraries) and basic Internet skills (97%), access to online health resources (76.8%), resources that aid visitors in finding better health insurance information (60%), and a place to complete online government forms (97%). In addition, public libraries are paramount in providing access to users who depend on free Internet access (100% of libraries) and Wi-Fi services (98%) to find information on building resumes, job searching, and interview preparation (73.1%). Public Library services are especially valuable to minority groups and low-income households, specifically in rural areas. Public libraries are viewed by individuals and families who utilize them as a reliable service that allows them to grow and are seen as environments that promote inclusivity and diversity (Alberg-Riger, 2019). Hispanics, African Americans and low-income populations in United States generally report that libraries are very helpful (Pew, 2015):34% of Hispanics believe they are beneficial in gaining workforce skills; 26% of households with an annual income of $30,000 or less agree; and 28% of African Americans echo this belief. Furthermore, public libraries have a history of advocating on behalf of users, specifically those from lower socio-economic communities and they are constantly working to protect users' ability to freely access information, thus enabling them to exercise their rights to intellectual freedom and to fully participate in a Democratic society through various resources and programs.

Therefore, the belief system that libraries are important to American communities' remains constant; in fact, library visits outnumbered trips to the movies in 2019 (Gallup, 2020). Studies show that public interest in libraries is among the highest for members of the Hispanic and Latinx communities, women, parents of minor children and older adults (Pew, 2015). For example, 78% of Hispanics believe that closing their library would significantly affect their communities. This is also true for 42% of Black users and 35% of low-income households who make $30,000 annually.

Thus, it is timely and critical that that we assess the state of technological measures and policies that public libraries may have in place to protect privacy of their patrons. The proposed forum will provide valuable information that will assist in creating a plan of action that will protect users' information and instill confidence in library patrons, thus preserving the legacy that libraries have created as a longstanding advocate for privacy rights and intellectual freedom and further enabling libraries to address and ameliorate policies that do not meet privacy standards for users.

The American Library Association (ALA) and Privacy Protections: The American Library Association has been committed to protecting privacy since its establishment in 1876. Through its Privacy Policy, Code of Ethics, and Library Bill of Rights, ALA sets the bar for the importance of information privacy and the roles libraries have in defending users' intellectual freedom and privacy rights. The ALA emphasizes that privacy is essential to libraries because it protects equal access to information. The ALA further asserts that libraries and library staff have an ethical obligation to promote equity and safeguard all users' personal information and history. ALA's Privacy Policy, last revised in May 2018, outlines how its organization and affiliates collect, use and share the information of users both automatically (e.g. Cookies, Web Beacons) and manually (e.g. Service Providers, Business Transactions, Lawful requests) with respect to the rights users have to the confidentiality of their personal information. The Privacy Policy developed by ALA ensures users' ability to restrict processing of their information, object to processing, or withdraw consent and emphasizes the role users have in deciding where and who their information is being shared to. In its most recent Code of Ethics and the Library Bill of Rights, updated in February 2019, the ALA includes a provision that stresses the importance of privacy for library users. Article VII says, "All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate about, and protect people's privacy, safeguarding all library use data, including personally identifiable information." The ALA encourages libraries to draft, adopt and revise library privacy policies as needed and offers guidance on how to strengthen library workers and users' understanding of the importance of information privacy.

Why Protecting Privacy is a Critical Aspect: The way we experience life and communicate with one another has been significantly influenced by technology as we evolve from a paper-based to a fully digital world (NIST, 2017). The endless possibilities of digital networks have given us an unprecedented sense of connectedness and opportunity for convenience that improves the way we communicate and interact and give us access to seemingly limitless information and resources. We are now able to communicate with each other instantaneously, download apps that connect to our cars and homes, and live a significant portion of our life through our phones and computers.

With the power of technology comes the responsibility to uphold a system of checks and balances that will limit the access that technology provides to our personal information. A fully accessible digital world, while beneficial, increases the likelihood that the right to personal digital privacy will be infringed upon. Maintaining digital privacy ensures that our personal information (e.g., passwords, banking information, health documents, other sensitive information) is safe from data collection or third-party users. Data collection and surveillance, especially, disregard our right to privacy in the name of national security (ACLU). This allows for an unparalleled invasion of privacy that can leave Internet users feeling helpless and unprotected. Surveillance gives the government and other entities the ability to personalize our online experience and cater to our interests, but it also allows insight into our private information and search histories that can be used against us and, in turn, hurt our personal or professional lives based on assumptions. This defeats the purpose of privacy and erases our ability to freely use the digital world without fear of giving away our personal information. Europe has recently developed a new legal framework that ensures data is gathered under stricter conditions and requires companies to protect any data that is collected from users. The ePrivacy Directive is built on existing frameworks that consider the fundamental right to privacy to ensure the best possible data protection (European Commission). In the United States, privacy as a human right is still a controversial topic. If the U.S. were to continue down the path of big data collection and surveillance, we could fall into a situation seen in Egypt in 2019, in which the authorities warned citizens that they would be closely monitoring online activity for signs of protesting and jailed those utilizing social media to interact with protests (AP News, 2019). While extreme, this would be a direct violation of United States' citizens First Amendment rights should government and company surveillance continue at this level. The concept of information privacy and how to understand and protect it is not yet concrete, which is why it is vital to continue researching the regulations and policies behind information privacy and how well these policies are protecting users in the United States. Most would agree that privacy is considered a "human right" (Huang, Bashir, 2015); however, there is a lack of technological measures and guidelines in place that completely secure the private information of users, specifically those who utilize public libraries.

As the digital world grows, the ability of librarians to defend the intellectual freedom and privacy of library patrons is being threatened. To combat this, libraries will work with third-party vendors to ensure privacy protections, often having to negotiate with these providers using guidelines provided by the American Library Association's (ALA) Code of Ethics. After further research, it was discovered that these privacy policies fail to meet the standards of the library community (Lambert, Parker, Bashir, 2015). Lack of adequate protection guidelines puts library patrons' right to intellectual freedom at risk. Studies have shown that public library usage is among the highest for low-income households and members of the Hispanic and Black communities (ALA). Libraries services, such as Internet and Wi-Fi, give free access to information that assists their communities in sending emails and texts, finding health resources, applying for schools and jobs, as well as other online services that users should be able to utilize without fear of involuntarily sharing personal information. This data suggests that low-income households and minority populations are more likely to lose their private information to data collection and hackers. Without reliable protection, users will likely turn away from library services because there is potential for someone else to view their reading history or access their confidential information (Caldwell-Stone, 2017). Libraries are also a key player in sustaining democracy and have strengthened democracy around the world (IFLA). Public library services have been paramount in providing equal access to information, enabling users to fully participate in their role as American citizens.

Project Design: This project, classified under National Digital Infrastructures and Initiatives, will draw on an advisory board that includes key stakeholders like: Privacy Enhancing Tech (PET) experts, public library directors/staff representing libraries of varying sizes (to ensure that small rural libraries as well as large/sophisticated ones are represented), members of the Library Information Technology Association (LITA), Library Freedom Project leads, representatives from recent NLG-L national forum grants that addressed library privacy, and members of the general public.

Therefore, this forum will allow for a meaningful discussion about public libraries and their role in protecting patrons' privacy with the goal of developing a unified solution to address this problem. Our project will be modeled after two prior National Forum grant-awarded studies: "A National Forum on Web Privacy and Web Analytics: Action Handbook" and "Library Values & Privacy in our National Digital Strategies: Field Guides, Convenings, and Conversations." whose respective PI's will join this project as collaborators to share information they have learned while working to fill the gap in protecting patrons' privacy.

The specific goal of this project is to create a forum in which public library professionals and privacy researchers can broadly discuss and evaluate how public libraries are protecting patron's privacy in our ever increasing digital world, while keeping in mind the historical leadership libraries have had in upholding such values. The objectives are to:

● Identify the current privacy protection practices among the various public libraries in the US
● Create a comprehensive set of current practices among various public libraries, including privacy protecting mechanisms and polices, and document challenges that public libraries are facing with emerging technologies, so that librarians, privacy experts, and stakeholders can better understand the wide spectrum of privacy protections across the public libraries.
● Engage with public librarians, technology companies, non-profit organizations, and researchers doing privacy related work to evaluate if such practices provide adequate privacy protections to its patrons given the challenges in digital privacy.
● Develop a guide that identifies public libraries' best practices and grand challenges in protecting patron's privacy, taking into consideration the variety of public libraries across the US. The guide will provide technical experts, funders, associations, and library partners with a clear view of the challenges public libraries face in protecting intellectual freedom, especially in relation to the library profession's increasing digital occupation.

To accomplish this, the project will organize a three-part forum to be held in the Fall of 2020, Midwinter 2021, and June 2021. The activities will be executed in three phases, a planning and development phase, a progress/feedback phase, and a reporting and dissemination phase

Proposed Timeline:

- November 19-21, 2020 – Part 1 of the forum willfocus on planning and development and will take place during the Library and Information Technology Association (LITA) Forum in Baltimore MD. The purpose of this initial meeting is to brainstorm on the best strategies for meeting the project's objectives and to identify key stakeholders to be included in the 2nd and 3rd phase of the forum.

- January 22-26, 2021 – Part 2 of the forum will take place at the ALA Midwinter Meeting in Indianapolis, IN and will present the evaluation plan and get feedback.
- February 2021 - May 2021 – During this time, the team will implement the assessment strategy, conduct the evaluation, and plan for final part of the forum
- June 2021 – Part 3 of the forum, which involves the second and final stakeholders' meeting, will take place at the ALA Annual Conference in Chicago and will present preliminary results from the evaluation and finalize outreach and distribution plans
- August 2021 – The final phase of the project includes drafting a final report and releasing a white paper that provides an overview of the best practices and grand challenges that public libraries faces in patrons' privacy protections

We will invite 30-40 experts but plan to host 20-25 experts who represent different voices and perspectives, drawing from individuals from the following areas:

Forum Event Planning and Preparation
IMLS funding will allow for inclusion of a diverse set of participants that will be invited from the lists provided below. We plan to utilize a combination of diverse perspectives, specifically from minority groups who are often underrepresented, to contribute to our research and forum goals. Participation from these individuals and groups is essential to the forum process and key to the success of this project. We are separating our prospective participants into four categories as follows:

I. Public Librarians, Library Administrators, Library Vendors, Library Funders
Librarians and other individuals and groups working in and around libraries are a staple in the success of our research. We aim to invite librarians and affiliates of public libraries who can provide valuable insight on a variety of key issues regarding information privacy. We also intend to invite a broad spectrum of professionals relevent to library operations who will provide crucial support for our research goals. We plan to invite: Shari Henry (Director at Roanoke County Virginia Library Association), Vickery Bowles (Toronto Public Library City Librarian and Executive Board Chair, Urban Libraries Council 2019-20), Rebecca Stavick (Executive Board Member, Urban Libraries Council), Jennifer Blenkle (Director of Strategic Initiatives, Urban Libraries Council), Susan Benton (President and CEO, Urban Libraries Council), Ray Hood (Chief Executive Officer, 3M Library Security/Bibliotheca), Matt Bellamy (President of Americas, 3M Library Security/Bibliotheca), Sarah Deutsch (Board Member, Electronic Frontier Foundation), Yan Zhu (Technologist Fellow, Electronic Frontier Foundation

II. Privacy Researchers, Activists, and Lawyers
This forum will provide our research with expertise from activists and researchers from ethnic caucuses, research groups, and diversity initiatives who focus on privacy issues related to public libraries. We intend to invite the following: Becky Yoose (Library Data Privacy Consultant, LDH Consulting Services), Deborah Caldwell Stone (Executive Director, Office for Intellectual Freedom and Editor, Journal of Intellectual Freedom and Privacy), Lana Adlawan (Representative, American Library Association Public Policy and Advocacy Office), Kathy Rosa (Director, American Library Association Office for Research and Evaluation), Shannon M. Oltmann (Principal Contact, Journal of Intellectual Freedom and Privacy), Michael Zimmer (Director, Center for Information Policy and Research), Emily Knox (Associate Professor,

School of Information Sciences at the University of Illinois at Urbana-Chamapign and Board Member, Association for Information Science & Technology, Beta Phi Mu, the Freedom to Read Foundation, and the National Coalition Against Censorship), Anne Craig (Senior Director, Consoritum of Academic and Research Libraries in Illinois), Bonnie Tijerina (Affiliate Researcher, Data & Society Research Institute), Erin Berman (Privacy Group Chair, American Library Association), Lori Bowen Ayre (Founder, The Galencia Group), Sam McBane Mulford (Facilitator and Strategist, The Galencia Group), Brian Behlendorf (Vice Chair of Board, Electronic Frontier Foundation), Teletha Brown (Head of Diversity and Inclusion Initiatives, Preservation of Electronic Government Information), Anne Craig (Senior Director, Preservation of Electronic Government Information), Kenny Garcia (President, REFORMA), Manny Figueroa (Chapter Representative, REFORMA), Richard E. Ashby, Jr. (President, Black Caucus Inc. American Library Association), James Allen Davis, Jr. (Executive Board Member, , Black Caucus Inc. American Library Association), Alanna Aiko Moore (President, Asian/Pacific American Librarians Association), Candice (Wing-yee) Mack (Vice President, Asian/Pacific American Librarians Association), George Gotts (President, American Indian Library Association), Heather Devine-Hardy (Executive Director, American Indian Library Association), Fu Zhuo (President, Chinese American Librarians Associations), Haiepeng Li (Associate Director, Chinese American Librarians Associations), Lian Ruan (Executive Director (Chinese American Librarians Associations), Minhao Zhang (Midwest Chapter President, (Chinese American Librarians Associations), Dr. Kenneth Yamashita (President, Joint Council of Librarians of Color and Former President, Asian/Pacific American Librarians Associations), and Alexandra Rivera (Vice President, Joint Council of Librarians of Color and Member, REFORMA), and Gladys Smiley Bell (Director at Large, Joint Council of Librarians of Color and Member, Black Caucus Inc. American Library Association). Other offices and groups to be invited: Office for Intellectual Freedom (Affiliate, American Library Association), Choose Privacy Every Day Blog (Office of Intellectual Freedom), Office for Research & Evaluation (Affiliate, American Library Association), and the Preservation of Electronic Government Information.

III. Designers and Developers
The systems we use to protect intellectual freedom and information privacy depend on those who design and maintain the systems. Including designers and project managers in our research will help us better understand and improve current and future systems and assist in the development process. We anticipate participation from: Ximena Diaz (Project Manager, Urban Libraries Council), Kelsey Henke, (Program Officer, Office for Research and Evaluation), Danielle M. Ponton (Program Manager, Round Tables of the American Library Association), Francis Alba (Project Assistant, Preservation of Electronic Government Information), and Jennifer Mascidrelli (Senior Project Management Coordinator, Preservation of Electronic Government Information).

Proposed Advisory and Collaborating Team:

Project Director – Masooda Bashir
Dr. Bashir is an Associate Professor at the School of Information Science at the University of Illinois at Urbana Champaign, and she will be the Principle Investigator and director of the project. See attached CV.

Key Project Staff – Yang Wang
Dr. Yang is an Associate Professor at the School of Information Science at the University of Illinois at Urbana Champaign. He co-directs the Social Computing Systems (SALT) Lab. He was previously an assistant professor in the School of Information Studies at Syracuse University and a research scientist in CyLab at Carnegie Mellon University. His research is centered around usable privacy and security, and social computing. His work has appeared in news media such as *The New York Times*, *Wall Street Journal*, BBC, and China Daily. His research has been supported by the National Science Foundation, Department of Health and Human Services, Google, Alcatel-Lucent, and The Privacy Projects. See attached CV.

Advisory Board & Collaborators:

Donna Pittman, Director, Champaign Public Library
Donna Pittman was appointed as the Director of the Champaign Public Library in 2016. Before her promotion, she was involved in several positions within the library, including serving as the Development Director.

Celeste Choate, Executive Director, Urbana Free Library
With over 24 years of experience in public libraries, Celeste Choate has earned her role as the Executive Director of the Urbana Free Library, where she currently serves a community of over 41,000 people.

William Marden, Director of Privacy and Compliance, New York Public Library
William Marden is the Director of Privacy and Compliance at the New York Public Library and is a certified information privacy professional. His research missions include identifying, implementing, and maintaining the New York Public Library's privacy policies and procedures. He also serves as the chair of the senior management Privacy Advisory Committee, conducts tests to assess information privacy risks, and champions the importance of information privacy by spreading awareness, offering training to employees, and working on the federal, state, and international levels to monitor and develop privacy laws and technology. See attached CV.

Joshua Stone, Director of Digital Services, Southeast Florida Library Information Network
Joshua Stone serves as the Director of Digital Services for the Southeast Florida Library Information Network. His research includes developing a network of privacy advocates in Southeast Florida. He is well-known for his advocacy for internet privacy and security, and he educates his community with classes that aim to inform patrons of risks. Joshua Stone also takes part in an online privacy project called the Library Freedom Project which aims to fight against surveillance and provide librarians with the proper tools to protect themselves and their patrons. His research also centers around implementing security measures for library users, specifically those facing social and economic hardships. See attached CV.

Becky Yoose**,** Library Data Privacy Consultant, LDH Consulting Services
Becky Yoose is a Library Data Privacy Consultant with LDH Consulting Services. Her research focuses on technology, metadata, and privacy, and is an integral part of understanding library data and administering library systems. She previously served as a Library Applications and Systems Manager at the Seattle Public Library where she contributed to the creation and

maintenance of policies related to privacy and security. Yoose has also obtained her license from the International Association of Privacy Professionals. See attached CV.

Scott Young, Associate Professor, Montana State University
Scott Young is an Associate Professor and User Experience & Assessment Librarian at Montana State University. His research focuses on topics in user experience and assessment of information services with a concentration in practical ethics and social justice. He also serves as an editor for Weave: Journal of Library User Experience and co-convener of the Digital Library Federation Privacy and Ethics in Technology Working Group, and he has hosted a National Forum on Web Privacy and Web Analytics. His goals are to assist libraries in helping more people. See attached CV.

Bonnie Tijerina, Researcher,Data & Society.
Bonnie Tijerina is a librarian who serves the library community by fostering communication between information management and e-resources professionals in libraries. In 2017, she was co-editor of an LITA Guide, *Protecting Patron Privacy*, and she most recently became an affiliate researcher at Data & Society where she focuses on facilitating projects concerning online privacy and ethics. Tijerina has extensive experience in libraries and the library community, dedicating ten years to creating opportunities for libraries and library patrons as the concern for privacy in the digital world grows.

Deborah Caldwell-Stone, Deputy Director, American Library Association.
Deborah Caldwell-Stone is the Deputy Director for the American Library Association. She has also served as interim director of ALA's Office for Intellectual Freedom (OIF) and executive director of the Freedom to Read Foundation. Her research and contributions center around working closely with library staff and affiliates on tackling intellectual freedom issues, censorship of library resources, government surveillance on library patron's privacy among other issues relating to information privacy. She has dedicated her career to advocating for intellectual freedom and privacy in libraries.

Michael Zimmer, Associate Professor, Marquette University
Michael Zimmer (PhD) is an Associate Professor in the Department of Computer Science at Marquette University. His research focuses on online privacy, the ethical dimensions of social media, libraries & privacy, and internet research ethics. Dr. Zimmer was recently appointed Editor of the ALA's Journal of Intellectual Freedom and Privacy. Current projects include PERVADE: Pervasive Data Ethics for Computational Research (NSF), Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems (NSF), and curating The Zuckerberg Files.

Note: We were unable to obtain letters of support from a preliminary set of stakeholder participants due to COVID-19 pandemic in the US and the ensuing closure of public libraries and related services. However, the project team has a wide network of professional contacts in the library profession, and we are confident that representatives from the various categories identified above will participate.

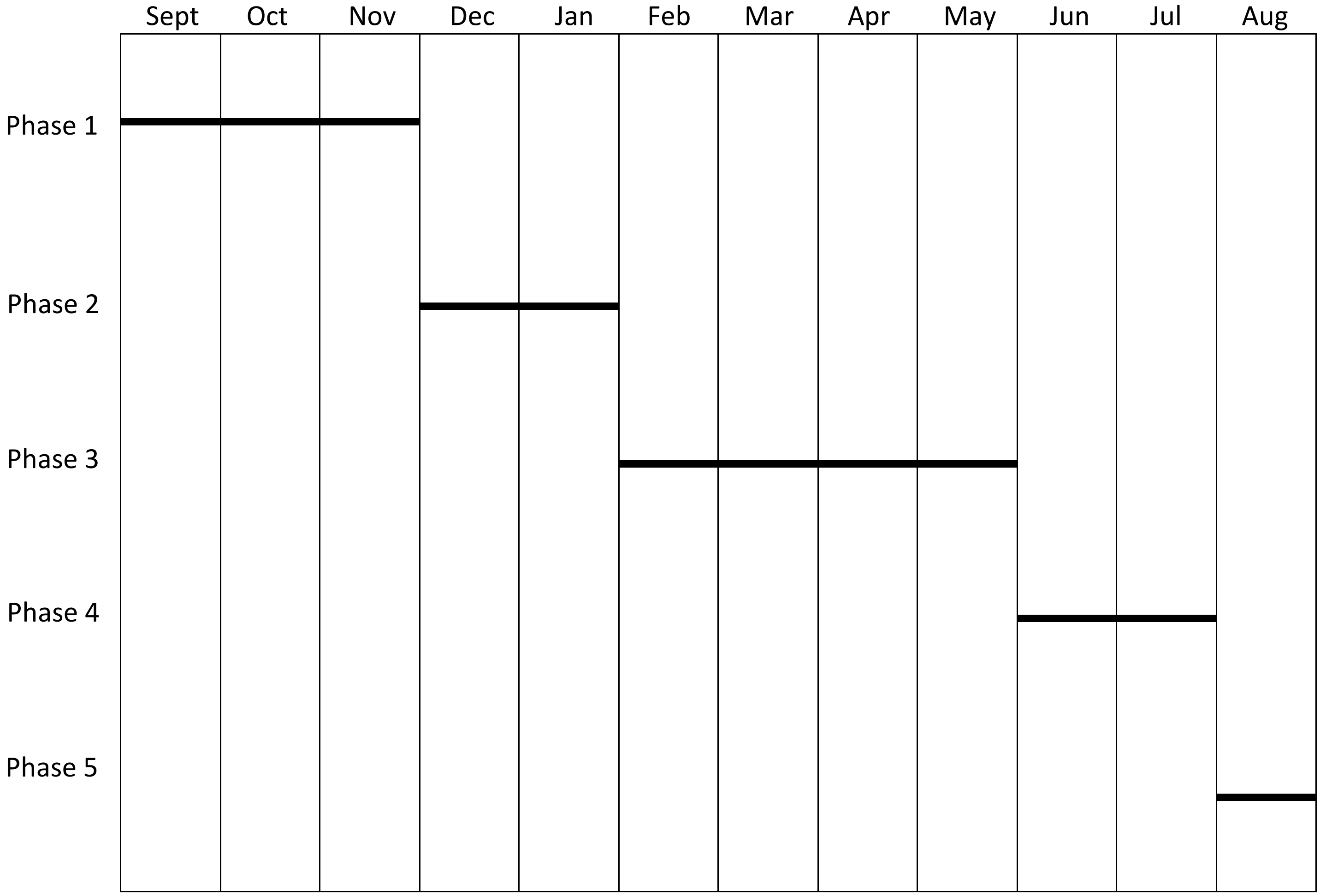
Diversity Plan: This forum is intended to showcase voices from underrepresented groups within the library community. Diversity and inclusion are a primary aspect of this project, and the perspectives of individuals from these communities will help ensure that the discussions and research accomplished will end in better outcomes with clearer results. To guarantee diverse views and bring forward an array of ideas, we will invite members from several ethnic caucuses (e.g, BCALA, REFORMA) to participate. Ethnic caucuses have been a cardinal force in advocating for and improving library services and resources for minority groups. We plan to utilize their expertise in supporting and improving library services for people of color to showcase the perspectives of those who are at a higher risk of losing their private information and to conclude with results that will allow us to implement new privacy measures and challenge and improve existing policies that do not meet libraries' standards.

Outreach and Dissemination Plan:

We intend to disseminate our findings through various means of scholarly publications. Potential publishing options include the Association for Rural and Small Libraries newsletter, which can provide citizens living in rural areas with more information on equal access and information privacy. The final white paper can also be distributed via multiple digital libraries and research databases, such as JSTOR or the Public Library of Science (PLOS), which is committed to offering the highest level of open access to all users, and will allow scholars, researchers and other individuals to access this information. In the information privacy community, there are several publication opportunities to pursue post-completion of this project, including The Privacy Project Newsletter, the Journal of Intellectual Freedom and Privacy, and the Choose Privacy every day blog,offered by the ALA's Office for Intellectual Freedom. These resources can provide a medium for easy access about the importance of information privacy to library users and non-users alike. Our outreach plan aims to educate the library community about the risks associated with the systems already in place to protect patron privacy and to promote use of research findings to move forward with more secure systems that will protect library users.

National Impact: While there have recently been valuable national forums that have explored library privacy, examining the privacy violations in web analytics and library values in the digital space, we see an important gap in the conversation about privacy and security technologies implemented in our public libraries in a broader sense. We also see a disconnect in the understanding and lack of shared vocabulary among the public library community and in differing levels of technical skillsets and resources across the wide range of public library systems. These shortcomings prevent consistent attention to this issue across the profession and hinder those responsible from building and deploying privacy protecting technologies in our libraries' hardware and software. There needs to be a systematic study in which key stakeholders discuss the status of patron privacy in our public libraries, what existing technology may or may not be appropriate to employ, and what new systems could be developed to help ensure the protection of patrons' privacy. To inform this discussion of what technologies are needed, therefore, it is essential that we have a national forum to focus on the adequacy of current practices and the extent to which they meet ALA guidelines.

Schedule of Completion
Proposed Timeline:



- Phase 1: September 2020 – November 19-21, 2020 – The first phase of the forum that will be focused on planning and development and it will take place at the Library and Information Technology Association (LITA) Forum in Baltimore MD. The purpose of this initial meeting is to brainstorm on the best strategies towards meeting the project's objectives and to identify key stakeholders to be included in the 2nd and 3rd phase of the forum.
- Phase 2: December 2020 – January 22-26, 2021 Part 2 of the forum will be at the ALA Midwinter Meeting in Indianapolis, IN to present the evaluation plan and get feedback.
- Phase 3: February 2021 – May 2021– Implement the assessment strategy and conduct the evaluation and plan for final part of the forum.
- Phase 4: June 2021 – July 2021 – Hold the second and final Stakeholders' meeting at the ALA Annual Conference in Chicago, present preliminary results from the evaluation and finalize outreach as well as the distribution plans.
- Phase 5: August 2021 – Final report and release of a white paper that provides an overview of the best practices and grand challenges that public libraries faces in patrons' privacy protections.

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.

The University of Illinois will hold rights and ownership to the resulting intellectual property but will not use them for commercial gain.

In order to maximize dissemination and reuse of project resources, all project resources will be assigned a Creative Commons License CC BY 4.0(CC-BY). The project team is committed to making all materials and resources available free of payment and access restrictions according to the terms of the CC BY 4.0 license. Resources will be made available through the project website, hosted by the iSchool at the University of Illinois at Urbana Champaign (UIUC). Project resources will be managed through UIUC Data banks and archived in IDEALS: http://ideals.illinois.edu.

For *research publications and presentations*, I will also use of CC BY4.0 license when possible. I will pursue publication and presentation in open access venues when possible.

For potential re-users, I will provide clear language on the license, attribution recommendations, and links to license details in our documents and website.

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.

The University of Illinois will hold rights and ownership to the resulting digital products but will not use it for commercial gain.
Project resources will be publicly available without any access restrictions. Use will be governed by a CC BY 4.0 license that will be noted on the materials. Published materials will be copyright by the authors and will be made open access via Ideals, the open access institutional repository at UIUC. https://ideals.illinois.edu.

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.

N/A

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.

Project resources will include a website, literature review, survey questionnaires to be completed by forum participants. Notes created during the forum, a white paper, a privacy protection technologies list, and conferences presentations and peer review publications. These resources will bedistributed and archived as HTML and PDF documents.

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 thework.

Standard web services and word processing software will be used to create project resources, including Google Docs, Microsoft Word, and Box Notes.

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 willcreate.

HTML, PDF

Workflow and Asset Maintenance/Preservation

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

The project will be led and managed by Masooda Bashir. Production and dissemination of project resources will also be led and managed by Masooda Bashir. Key personnel Yang Wang will provide support throughout the duration of the project. The advisory board members and collaborators listed will be invited to the first forum so they can provide feedback for the overall forum planning phase2 &3 and the stake holders that should be included in the different phase of the forum.

B.1 Describe your plan for preserving and maintaining digital assets during and after the award period.

Resources will be made available through the project website, hosted by UIUC, with project resources managed through Illinois Data Bank for Shareable resources and archived in IDEALS, the open access intuitional repository at UIUC. http://ideals.illinois.edu.

B.2 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).

Project staff will be responsible for maintaining the digital content for the duration of the grant and depositing the materials into IDEALS, the institutional repository of the University of Illinois at Urbana-Champaign, for long-term preservation and access.

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).

Metadata will be produced in the IDEALS and Illinois Data Bank repository interfaces. IDEALS repository complies with DublinCore, OAI-PMH, among other standards (see https://wiki.illinois.edu/wiki/display/IDEALS/Metadata+Policy). Illinois Data Bank complies with DataCite standard.

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

Both UIUC's IDEALS repository and Illinois Data Bank will support metadata beyond the grant period.

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).

Both UIUC's IDEALS repository and Illinois Data Bank provide a GUI and API for search and discovery. The PI and research staff will promote them to professionals at conferences, meetings, and other communication channels.

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).

Assets will be available online through the project website via standard web browsers as well as deposited in IDEALS repository, using DSpace, and Illinois Data Bank, based on Ruby on Rails application.

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.

Illinois Data Bank: https://databank.illinois.edu/datasets
IDEALS: https://www.ideals.illinois.edu/handle/2142/150

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.

N/A

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.

N/A

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.

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

N/A

Access and Use

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

N/A

C.2 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:

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.

After Phase1, the project we will use survey, qualitative interviews, and focus group methods to collect data. This data from these methods will serve as an essential part of what will create the white paper at the end of the project.

All data collected throughout the phases of the project will contribute to scholarly publications and presentations.

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 project will require approval and oversight by the UIUC's Office for the Protection of Research Subjects.

IRB Approval will be sought and secured before the project start for the surveys, interviews, and focus groups which will take place after Phase1 has been completed. Phase2 and other phases includes only straightforward, minimal risk studies, and the PI has extensive experience in running IRB approved human subject studies. The PI and/or research staff will design waiver of consent for the online surveys but will collect and document consent when doing interviews/focus groups. Printed/paper records will be kept in paper format in a locked file cabinet in the PI's office, for at least 3 years from the study's. For these participants, a key of unique identifiers will be the link between consent/permission/assent documentation and study responses. This key will be password protected and only accessible to the PI and research staff.

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.

No. The forum study methods do not require or need to collect sensitive information. However, the project will store data on secure machines with password protection, and only project staff will have access to them.

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

Survey data will be captured via Qualtrics web survey software and exported in .csv format, which can be readable by many statistical and spreadsheet applications. Qualitative data will be captured via audio recorders. Audio files will be downloaded to secure machines, password protected, and transcribed into .docx and .pdf formats. Any field notes of observations taken by the PI or research staff will be generated and maintained in .docx and .pdf formats. These will also be password protected. Across the project, only the PI and the research staff will have access to raw 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?

Codebooks, code reports, and project notes will be created and stored on local, secure machines in .docx and .pdf formats. Documentation will include identifiers for data collection type (e.g., stakeholder survey, focus group) and participant as needed.

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

We will deposit any shareable data sets and data products into the Illinois Data Bank for long term preservation and dissemination.

A.7 Identify where you will deposit the data:

Name of repository: Illinois Data Bank

URL: https://databank.illinois.edu/

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

This data management plan will be reviewed at each phase of the forum with project staff. The PI will monitor the compliance with the plan as well as makes modifications to the plan to accommodate project developments or technological advancements.