Digital Shred: Case Study of a Remote Privacy Literacy Collaboration

Sarah Hartman-Caverly, Alexandria Chisholm, and Alexandrea Glenn

This qualitative, evaluative case study details the conceptual framing, development, delivery, and assessment of a privacy literacy workshop called Digital Shred. The workshop is a multi-institutional effort offered initially in-person in fall 2019 and adapted to virtual delivery in fall 2020. The conceptual framework underlying the workshop includes reputation management, behavioral surplus, data doubles, data governance, and information security damage assessments. Learning outcomes and activities were inspired by inclusive, responsive, active learning pedagogy. Anonymous formative assessment feedback suggests that participants are motivated by the personalized learning activities and value this theory-informed approach to privacy literacy.

Introduction

Privacy literacy, understood as "a suite of knowledge, behaviors, and critical dispositions regarding the information constructs of selfhood, expressive activities, and relationships," is a growing opportunity for information literacy instruction in academic libraries.[1] Privacy literacy instruction presents the positive case for privacy in the human experience, and seeks to enhance technosolutionist privacy training that focuses on front-end privacy settings and technologies by cultivating students' capacities for situational awareness, critical thinking, self-reflection, and judgment. Informed by student-centered learning design, privacy literacy instruction can also resist a prescriptive or proscriptive approach to privacy and technology use in order to respect students' autonomy, values, and lived experiences.

Americans are increasingly attuned to the risks and disparate harms of personal data tracking, surveillance, profiling, and behavioral nudging, and awareness of these phenomena has inspired renewed interest in privacy and privacy-protecting strategies.[2] Privacy toolkits are available from organizations dedicated to civil liberties and press freedoms, including the ACLU, Electronic Frontier Foundation, Electronic Privacy Information Center, and Freedom of the Press Foundation.[3] In the library space, Library Freedom offers privacy-related professional development and resources, and San Jose Public Library's self-paced Virtual Privacy Lab is an exemplary public library-based initiative.[4] The American Library Association recently amended

* *Sarah Hartman-Caverly is Reference and Instruction Librarian at Penn State University, email: smh767@psu.edu; Alexandria Chisholm is Reference and Instruction Librarian at Penn State University, email: aec67@psu.edu; Alexandrea Glenn is Student Engagement Librarian at the University of Pennsylvania, email: reaglenn@upenn.edu.*

the Library Bill of Rights with the addition of article VII, which calls on libraries to "advocate for, educate about, and protect people's privacy."[5] In academic librarianship, awareness of privacy and the commodification of personal data feature in the Information has Value frame of the ACRL Framework for Information Literacy for Higher Education, and privacy literacy is identified as an emerging literacy in the ACRL 2021 Environmental Scan.[6]

This qualitative, evaluative case study details the conceptual framing, development, delivery, and assessment of a co-curricular privacy literacy workshop, the Digital Shred Workshop. The Digital Shred Workshop was collaboratively developed and delivered by librarians at two R1 research universities. Reputation management, behavioral surplus, data doubles, data governance, and information security damage assessments are introduced as the conceptual framework for the workshop. After discussing the conceptual framework for the workshop, the article will present additional details on institutional context, a detailed description of the learning experience, and results of a formative evaluation. The case study concludes with resources, lessons learned, and future directions for developing library-led privacy literacy programming.

Literature Review

Prevailing approaches to privacy literacy in academic libraries focus on privacy in the digital or online context, highlighting behaviors, settings, and tools that patrons can adopt to better protect their privacy. Rotman proposes a privacy literacy framework as a complementary literacy to digital literacy.[7] Rotman's privacy literacy framework for online interactions includes five elements: *understanding* the characteristics of information, *recognizing* online social interactions as potential privacy threats, *realizing* the possible outcomes of online information disclosure, *evaluating* privacy threats in a given online interaction, and *deciding* on how and when to disclose information online.[8] Wissinger demonstrates alignment between Rotman's privacy literacy framework and critical thinking definitions to further inform privacy literacy instruction.[9] Lowe argues that privacy and online security should be included in information literacy instruction, and Tewell advocates the inclusion of privacy in critical information literacy learning experiences.[10] Wharton notes that privacy literacy can be delivered in conjunction with digital literacy and digital citizenship programming, and provides examples of digital privacy educational offerings from academic libraries.[11] Wittek suggests specific privacy literacy instruction topics, including demonstrating alternative search engines, browser extensions, and temporary email accounts, as well as advising patrons to consider the privacy implications of apps and cloud storage used for research.[12] Hartman-Caverly and Chisholm find that data profiling and consumer privacy topics are most commonly featured in privacy literacy instruction, which pays less attention to surveillance and intellectual freedom concerns.[13] Project Information Literacy reports that many students make deliberate decisions with respect to online disclosure and privacy protections, and recommends that students learn about the privacy-related concept of algorithmic justice.[14]

Hagendorff offers four critiques of common approaches to privacy literacy.[15] First, Hagendorff observes that unequal access to privacy literacy learning experiences perpetuates the disparate impact of surveillance and profiling on members of vulnerable and marginalized groups. He notes that differences in privacy knowledge are observed along lines of educational attainment, income, age, race and ethnicity, and gender identity.[16] Second, Hagendorff questions the presumption that users are purely rational actors with respect to privacy and disclosure, noting that there is often no meaningful choice between practicing one's privacy values and gaining access to basic necessities of life. Project Information Literacy finds that students experience both resignation and indignation in the face of what Barassi terms "*systemic coercion of digital participation*."[17] Third, Hagendorff finds fault with the front-end focus of privacy literacy approaches that impart on users a false sense of control over their consciously given data by failing to address backend processes underpinning automatically monitored and modeled data.[18] Finally, Hagendorff criticizes what he terms responsibilization, or the shift of responsibility for privacy onto end users and away from major corporate and state entities.[19]

Informed by these critiques, Hartman-Caverly and Chisholm propose privacy literacy instruction informed by a conceptual model centered on the positive role of privacy in the human experience, rather than on data flows or digital technologies.[20] Their privacy literacy efforts highlight the role of privacy in *identity*, *intellect*, bodily and contextual *integrity*, *intimacy*, social *interaction*, and voluntary *isolation*, noting that privacy is about respect for persons—not just protection of data.[21] Responding to Hartman-Caverly and Chisholm's call for increased scholarly communication about privacy literacy efforts in academic libraries, this qualitative, evaluative case study examines an original privacy literacy workshop designed with these principles in mind.

Research Questions and Methods

This article reports on a qualitative, evaluative case study examining a novel approach to privacy literacy instruction.[22] It delivers an in-depth exploration of the theory, goals, design, implementation, and results of an original privacy literacy workshop, developed collaboratively and delivered at two academic institutions. Authors implemented Simons's qualitative case study methodology as depicted in table 1, which involves conceptualizing the topic, defining the case and identifying the unit of analysis, framing research questions and issues, and gathering and analyzing data.[23] Authors conceptualize the topic as privacy literacy instruction in academic libraries, and define the case as a new, original privacy literacy workshop developed and delivered by librarians at Penn State Berks (PSU Berks) and University of Florida (UF) in fall 2019 and adapted for virtual delivery in fall 2020. The research questions explored are:

- How did librarians respond to Hagendorff's four problems with privacy literacy in workshop design?
- How did librarians integrate privacy theory into workshop learning activities?
- How successful was the workshop in engaging participants to achieve learning outcomes?
- What lessons learned are generalizable to other privacy literacy efforts in academic libraries?

Data gathering strategies include document analysis, observation, and anonymous assessment data collected on an opt-in basis. Document analysis was performed by each author separately on notes from planning meetings, related email threads, and iterative drafts of lesson plans and learning activities. Observations from three workshop sessions were gathered through peer teaching observation and instructor self-reflections. Anonymous formative assessment data was collected from participants in culminating reflection questions and analyzed for common trends and idiosyncratic responses. Analysis is evidenced by an accounting of the workshop's development, peer teaching observation, qualitative thematic analysis of anonymous participant feedback (including from students, faculty, and staff), and reflections of the workshop developers and facilitators.

Table 1 demonstrates how authors implemented Simons's evaluative qualitative case study methodology to answer research questions about their original privacy literacy workshop.

TABLE 1
Simons's Case Study Methodology

Conceptualize the topic	Privacy literacy instruction in academic libraries.
Define the case; specify the unit of analysis	A new, original privacy literacy workshop, Digital Shred, developed and delivered by librarians at PSU Berks and UF in fall 2019 and adapted for virtual delivery in fall 2020.
Frame questions and issues	• How did librarians respond to Hagendorff's four problems with privacy literacy in workshop design? • How did librarians integrate privacy theory into workshop learning activities? • How successful was the workshop in engaging participants to achieve learning outcomes? • What lessons learned are generalizable to other privacy literacy efforts in academic libraries?
Gather data	Document analysis was performed independently on notes from planning meetings, email threads, and iterations of lesson plans and learning activities. Observations from three workshop sessions, one in-person in fall 2019 and two virtual in fall 2020, were gathered in the form of peer teaching observation and instructor self-reflections. Anonymous formative assessment data was collected from participants in culminating reflection questions and analyzed for common trends and idiosyncratic responses.

Institutional Context and Collaboration

The Digital Shred privacy literacy workshop is the product of a multi-institutional collaboration between two instructional librarians at Penn State Berks Thun Library and a student success librarian at University of Florida Smathers Libraries. As context for the workshop case study, this section provides background on the participating institutions, origin and facilitation of the collaboration, and pedagogical philosophy and lesson planning activities.

Thun Library is an information commons, free-standing collection of more than 50,000 volumes, and an instructional unit within Penn State University Libraries system serving the Penn State Berks campus. Penn State Berks is a public, partially residential, regional liberal arts college and Commonwealth Campus of the Pennsylvania State University, offering more than twenty degree programs to approximately 2,500 students in the greater Reading City and Berks County region of the state.[24]

Thun Library is also home to established co-curricular privacy literacy programming, the Penn State Berks Privacy Workshop Series.[25] These one-hour privacy literacy learning experiences focus on privacy issues for students in the past, present, and future. At the time of the development of the Digital Shred Workshop, the series comprised an introductory Privacy Workshop, spotlighting personal and societal privacy practices in the current environment; and a Digital Leadership workshop, exploring future implications of individuals' digital behaviors. Digital Shred, the subject of this case study, provides tools to evaluate and mitigate the damage of past digital behaviors. After the addition of Digital Shred, PSU Berks librarians developed a fourth workshop, Digital Wellness, to focus on privacy across the lifespan, bringing together the past, present, and future by finding a balance of technology and wellness while aligning habits and goals. The Privacy Workshop is integrated into first-year seminar programming, while the Digital Leadership, Digital Shred, and Digital Wellness workshops are offered as free-standing, co-curricular learning experiences in partnership with the Campus Life Office as well as Career Services, College-wide Reading, and Counseling Services. These cross-campus partnerships contribute a great deal to the success and participation rate of the workshops through collaborative outreach and promotion.

Smathers Libraries, with a total collection of more than six million print volumes, serve the University of Florida, a public, primarily residential, national R1 research university offering 100 undergraduate majors and 200 graduate programs to approximately 50,000 students located near Gainesville in northern Florida.[26]

This multi-institution privacy literacy collaboration resulted serendipitously from networking at professional development events. During a preliminary conference call, the three librarians established a shared interest in developing a workshop focusing on rationales and techniques for personal data governance. The workshop was scheduled to pilot at PSU Berks in fall 2019 as part of an existing Privacy Workshop Series, then comprising the foundational Privacy and Digital Leadership workshops. The collaborators agreed to apply the principles of consensus-building and backward design to their work.[27] The PSU Berks librarians shared their existing workshop materials and some highlights from their recent literature review on privacy literacy to support the new collaborator in building foundational knowledge.

Working backward from the workshop pilot date, collaborators scheduled a series of Zoom meetings, each with its own purpose and deliverables. To preserve the integrity of individual insights and creative ideas, collaborators committed to develop content independently, and then share and synthesize materials during conference calls. After crafting learning outcomes for the workshop, each contributor proposed and independently developed learning activities, and the team reached consensus on a definition for "digital shred" as "the act of managing privacy by curating digital records for purposes of data governance, risk management, and storage efficiency."[28] A final meeting was scheduled to review and finalize workshop materials, populate the workshop guide, and discuss the flow of the workshop from one learning activity to the next. These learning activities, their implementation, and participant responses are explored in more detail in subsequent sections.

Conceptual Framework

The Digital Shred Workshop is informed by the concepts of reputation management, behavioral surplus, data doubles, data governance, and information security. Reputation management developed as a concept in business and strategic communication; more recently, it is used to describe how digital citizens construct their online presence and perform varied personal identities intended for different audiences across a range of social contexts.[29] Reputation management is a common focus of privacy literacy instruction in academic libraries, in which librarians discuss the negative personal and professional consequences of social media misuse. Related learning outcomes for these privacy literacy learning experiences include strategies for students to adopt privacy-friendly technologies, maintain protective privacy settings, and exercise judgment in their social media use.[30]

While important, privacy literacy instruction focused exclusively on reputation management behaviors may obscure the hidden harms of platform surveillance and overstate the ability of users to control their personal data flows, contributing to the control paradox.[31] Information on behavioral reputation management can be complemented with a discussion of behavioral surplus, the automatically monitored metadata that users generate when they interact with networked technologies, including things like "websites visited, psychographics, browsing activity, and information about previous advertisements that the user has been shown, selected, and/or made purchases after viewing."[32] Sometimes referred to with seemingly innocuous terms like data trails or digital exhaust, behavioral surplus is personal data that users do not consciously provide and over which users can exert very little control. Behavioral surplus is routinely combined with consciously given data and processed with machine learning to generate profiles of modeled data about individual users. These data doubles are employed to assess and predict attributes about individuals, from attractiveness to trustworthiness.[33] Data doubles not only shape individuals' online experiences, such as by informing the display of personalized advertisements, the relevancy ranking of search results, or the output of recommender systems, but also increasingly impact their real-world experiences, including suggested matches in dating apps, access to financial credit, hiring decisions, and sentencing in the criminal justice system.[34]

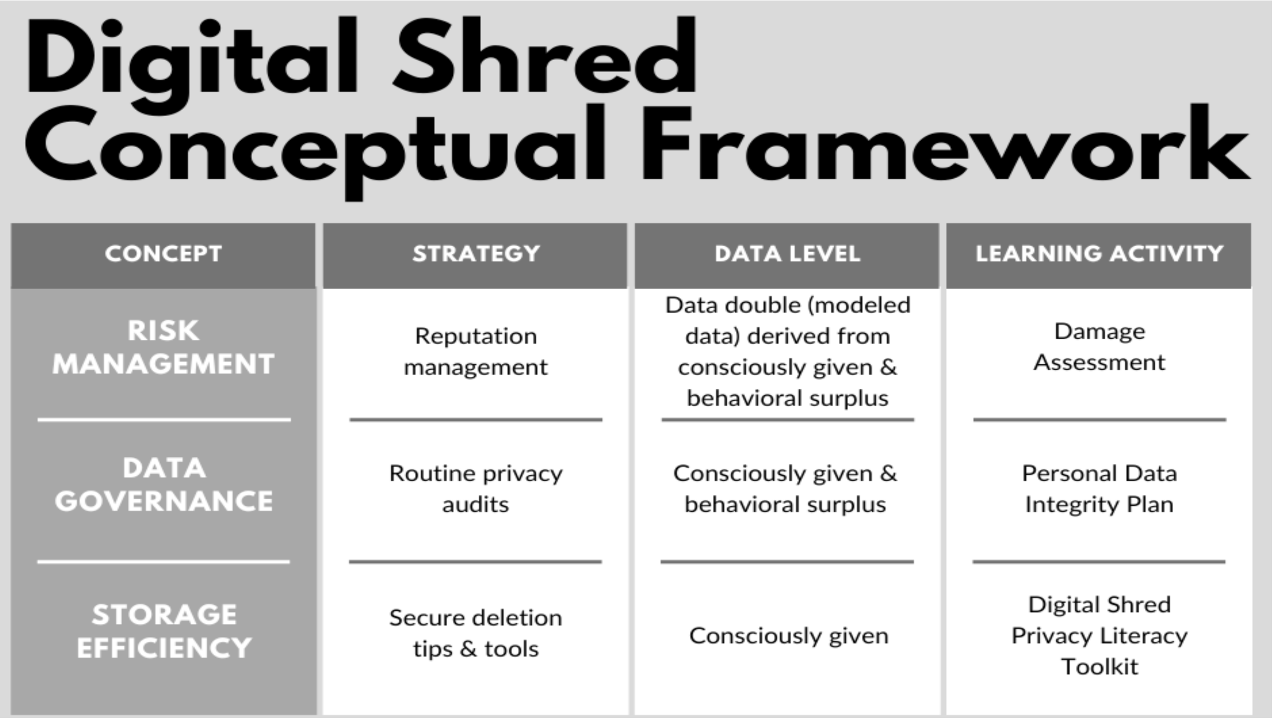
The authors seek to empower students with actionable information in privacy literacy instruction while honestly acknowledging individual users' limited ability to influence the collection of behavioral surplus or escape the shadows of their data doubles. To achieve this, the concept of data governance is adapted from its information science context to refer to data management strategies that preserve data accuracy, utility, and security.[35] Data governance takes a holistic view of managing the data lifecycle, including recognizing when data is no longer useful or may even become a liability, and securely destroying such data. One technique for identifying and managing high-risk data assets is to undertake an information security damage assessment, which evaluates the actual or potential harm resulting from unauthorized access to or use of sensitive information.[36]

The conceptual framework for Digital Shred applies the strategies of risk management, storage efficiency, and data governance to privacy literacy, as summarized in figure 1. Risk management is addressed in the context of reputation management, including a damage assessment of participants' data doubles. Their data doubles comprise modeled data generated by machine learning processes applied to their behavioral surplus (or automatically monitored data) combined with their consciously given data. Storage efficiency is achieved through the secure deletion of participants' consciously given data on a targeted basis, informed by their damage assessment results. Participants are further made aware that behavioral surplus is generally beyond the user's control, and often cannot be actively managed or deleted except by making requests of data brokers, profilers, or platforms. Data governance is informed by routinizing privacy audits through a personal data integrity plan.

Figure 1 summarizes the authors' conceptual framework for their original Digital Shred privacy literacy workshop.

The Digital Shred Workshop introduces participants to the concepts of behavioral surplus and data doubles, and how they can impact not only reputation but also access to information and opportunities. The workshop also imparts strategies for reputation management based on data governance and damage assessment techniques, using secure file shredding as a metaphor for the proactive management of one's digital dossier. Participants are provided with

FIGURE 1
Conceptual Framework for Digital Shred



Digital Shred Conceptual Framework

CONCEPT	STRATEGY	DATA LEVEL	LEARNING ACTIVITY
RISK MANAGEMENT	Reputation management	Data double (modeled data) derived from consciously given & behavioral surplus	Damage Assessment
DATA GOVERNANCE	Routine privacy audits	Consciously given & behavioral surplus	Personal Data Integrity Plan
STORAGE EFFICIENCY	Secure deletion tips & tools	Consciously given	Digital Shred Privacy Literacy Toolkit

decision-making frameworks and tools for determining their own online persona priorities, articulating areas of risk, identifying compromised and defunct digital accounts, and shredding some of their digital baggage.

Digital Shred Learning Experience

As a new offering in an established privacy workshop series, the Digital Shred Workshop was designed to scaffold into a more extensive learning experience. Within the larger series, the Digital Shred Workshop serves as the most traditional privacy literacy learning experience—one which addresses tactics and practical tools to protect individuals' privacy and security. However, the authors' commitment to theory-informed teaching means countering approaches that overpromise user control in the face of information asymmetries and the control paradox, and that embrace students' autonomy and agency by avoiding prescribed solutions.[37] This teaching philosophy is nearly antithetical to the traditional technosolutionist privacy workshop model, which promises participants access to foolproof methods to protect their privacy with front-end features such as customizing privacy settings, installing browser plug-ins, or setting a strong password, and thus requires a creative approach.

In order to embrace the authors' understanding of privacy literacy while still offering participants practical options to safeguard their privacy, emphasis was placed on encouraging decision-making frameworks. Employing backwards design, learning outcomes were collaboratively established early in the process to guide development of workshop activities and micro-lecture content:

Participants will be able to:

- reflect on and describe their digital privacy priorities in order to articulate the benefits and risks of their digital dossier.

- apply a growth mindset to critically examine their current data double and recognize when change is needed.
- develop a Personal Data Integrity Plan that makes routine the process of auditing and updating their digital dossier in alignment with their privacy values.
- describe "digital shred" and its importance.

At PSU Berks, this co-curricular workshop is a part of the larger Privacy Workshop Series and as such must operate as both a freestanding and integrated workshop. Much like other workshops in the series, a variety of active learning activities are implemented with a mix of opportunities for individual metacognitive reflection and large group discussion for contextualization. No prior knowledge is required, but efforts to scaffold content to a first-time attendee, or to deliver Digital Shred as a standalone workshop, are necessary. The workshop begins with a gamified prior knowledge check to scaffold the Digital Shred Workshop for any participants who did not attend the foundational privacy workshop. The authors' developed a Kahoot quiz using "fact or fiction" statements, as seen in appendix A. As instructors move through the quiz, they provide brief explanations and context as to why each statement is fact or fiction. In total, this assessment takes about five minutes to implement.

Next, instructors present a short five-to-ten minute microlecture covering vital concepts. Instructors briefly define "digital shred" as it relates to the concepts of data governance, data minimization for risk management, and storage efficiency. The microlecture concludes with a brief overview of "data doubles,"[38] bridging content from the Privacy Workshop with the Digital Shred Workshop. Students encounter their data doubles, modeled data which results from the aggregation and analysis of consciously given data and behavioral surplus using big data techniques, like algorithms and artificial intelligence. Facilitators explain that modeled data is used to calculate things like quantified attractiveness in dating apps, or trustworthiness for employability purposes, and can affect real-life opportunities and experiences.[39] To transition from the microlecture into workshop activities, facilitators suggest that adopting digital shred practices aids users in managing their "data double" or modeled data.

The first activity uses character development conventions and reputation management concepts to create a "perfect persona," which allows students to determine what behaviors they deem most impactful for maintaining their digital privacy. Students often have their own understanding of how intrusive big tech can be,[40] but asking them to articulate their privacy values helps them to define their personal privacy priorities. Creating a perfect persona lets students determine what behaviors they deem the most beneficial for maintaining both digital presence and digital privacy. Instructors introduce the Ideal Portfolio worksheet, in which participants develop a "burner account," as seen in appendix B. The worksheet begins with a general prompt:

> If you were creating a perfect account (or a fake burner account to do private research on a crush), what would you choose to make it a perfect account? From username to posted content, what would you consider ideal?

Students then create this idealized portfolio by responding to guiding questions, such as crafting an ideal username and bio; determining what email address or phone number to use to register the account in light of doxing risks; strategizing online interactions such as liking, sharing, posting, and following; and planning the timing and frequency of their postings, including whether to share locational data. Instructors then facilitate a large group debrief regarding the qualities of an ideal digital portfolio and the audiences students have in mind for their digital portfolios, unpacking rationales for their choices. Of all the activities, this worksheet involves the least sensitive information and, in the authors' experience, garners the most open discussion amongst participants.

After the debrief, the Damage Assessment activity is introduced. The Damage Assessment worksheet, adapted from the protocol used by US intelligence agencies to assess the impact of a sensitive information breach,[41] provides a structure for participants to evaluate actual or potential damage resulting from infiltration or exfiltration of their online accounts, identify systemic vulnerabilities, and develop a corrective action plan, as seen in appendix C. Like the ideal portfolio activity, the Damage Assessment opens with a prompt:

> Imagine your personal accounts were infiltrated by a hostile intelligence asset (or maybe just your kid sister) who exfiltrated sensitive information about you! Use this framework, adapted from Intelligence Community Directive 732: Damage Assessments, to identify your risks and plan corrective actions.

Worksheet questions prompt participants to consider their risky digital behaviors, from storing passwords in a browser to sensitive web browsing; to identify the types of high-risk personal data generated by their online activities; to estimate the damage caused by a worst-case scenario personal data breach; to assess the risk or likelihood of a personal data breach occurring; and to plan corrective actions to minimize risk.

After allowing participants time to work independently on their personal damage assessments, instructors once again facilitate a large group discussion, inviting students to share their thoughts, reflections, and findings from the activity. This damage assessment activity is primarily intended to support individual students' metacognition and critical reflection, and to benefit them personally at their privacy point of need. Due to the sensitive nature of these topics, students are invited to share general observations but are by no means cajoled or coerced into sharing any of their personal reflections. It can be helpful to have generic or instructor-specific examples ready to share in lieu of student participation. The combined Ideal Portfolio and Damage Assessment activities and large-group discussions take approximately fifteen minutes.

The workshop culminates in the Personal Data Integrity Plan, a data governance tool inspired by privacy audit practices,[42] as seen in appendix D. To set the stage for the activity, students explore a series of interactive links, including general breach-monitoring tools like Have I Been Pwned?,[43] to review their own digital footprints in real time. The list also contains links to Blacklight, a tool which scans websites for user-tracking technologies, and instructions on how to create a personal Google search alert for reputation management purposes.[44] Students particularly enjoy investigating Have I Been Pwned? where they often search not only for their own accounts but also their loved ones' emails, namely their parents.

After students review these tools, instructors introduce the worksheet and accompanying resources. The Personal Data Integrity Plan worksheet identifies common areas of privacy risk and technology use, such as Smartphone, Web Browser, Social, Productivity and Organization, Health and Wearables, and Smart Home. Within each category, specific products, platforms, or operating systems are listed so that students can select the ones they actively use, with space to write in custom responses. Participants then assess their personal risk level for each product as high, neutral, or low, based on their reflections from the Ideal Portfolio and Damage Assessment activities. Finally, informed by this risk assessment, participants determine the frequency with which they want to audit these accounts for privacy risks, or can opt to mark them for deletion altogether. Resources are linked from the worksheet to support participants in the digital shred of their "zombie" accounts, sensitive personal data, and other high-risk online content.

To alleviate the burden of creating and regularly updating how-to documents, the PSU Berks librarians created an online toolkit to support learning activities through curated, existing online content.[45] Instructors leverage the Digital Shred Privacy Literacy Toolkit to link out to "How-to" resources that provide steps on mitigating and reducing privacy and data security harms. This allows the students to independently use several resources to critically evaluate their own digital footprint in real time. Categorization of the "How-Tos" content of the Digital Shred Privacy Literacy Toolkit complements the sections of the Personal Data Integrity Plan (i.e., Smartphone, Web Browser, Social, Productivity and Organization, Health and Wearables, and Smart Home). For example, the Smartphone category includes how-to guides on enabling password locks and two-factor authentication, installing a VPN, deleting sensitive data from cell phone photos, minimizing locational data tracking, using DuckDuckGo for navigation, removing zombie apps, and updating privacy settings for Android, Google, and iOS devices. This approach enables greater flexibility and opportunity for personalization, since technology is constantly evolving, and the authors' goal is to allow students' own privacy concerns to direct this learning activity. On a practical note, it is useful to provide a curated list of highly relevant, direct links in a workshop guide, with additional longer lists of categorized resources (linked from the creators' toolkit) available through the worksheet. This approach respects students' agency and autonomy by creating an atmosphere in which the activity is driven by the priorities and values they articulate, while still receiving guidance and direction.

Students work independently on the Personal Data Integrity Plan for about fifteen minutes, and instructors then take time to conduct a brief large group discussion, allowing participants to ask questions or share observations. The ultimate goal of the workshop is for each student to leave with at least one behavioral change or corrective action that will help limit their digital footprint, and, hopefully, a fresh perspective on privacy.

The Digital Shred session concludes with "snowball confessions,"[46] a gamified method of formative self-assessment, culminating in a discussion of what participants have learned. Instructors provide each participant with a scrap paper. Participants are asked to respond to at least one query among three optional prompts, then crumple up their paper and throw it into the center of the classroom for another attendee or an instructor to share aloud. This kinesthetic assessment method enables personal reflection and large group discussion while ensuring participants' anonymity. Optional prompts included:

- What is one change and/or step you plan to take after this workshop?
- What is one bad digital habit you want to break?
- List something you learned today OR something you wish you had learned.

As an anonymous, gamified, formative self-assessment, snowball confessions offer a final opportunity for metacognition and large group discussion while also respecting participants' privacy and privacy values.[47] Snowball confessions further give workshop instructors valuable insight into the student learning experience. The workshop assessment does not seek to measure participants' behavioral change against a predetermined benchmark, since the instructors' teaching philosophy purposely avoids prescribing or proscribing specific behaviors with respect to privacy and technology use in the interest of respecting students' autonomy and intellectual freedom. Additionally, because facilitators view the cultivation of privacy literacy as both highly personal and a continuous work-in-progress, formative self-assessment is better aligned with understanding how students experience the workshop learning activities in relation to their own privacy values, rather than administering a summative assessment to test their recall of specific workshop concepts.

Participant Response

The Digital Shred Workshop was piloted at PSU Berks in November 2019, and then adapted for virtual delivery at both PSU Berks and UF in the 2020–21 academic year, reaching a total of fifty participants at the time of writing. Six students attended the pilot Digital Shred Workshop in-person at PSU Berks in November 2019. Despite the small audience, a wide range of self-reported student demographics were represented; these included three non-traditional students and three traditional college age students, consisting of three first-year students, three upper-level students, one international student, and one student veteran. The authors formatively assessed the workshop by asking participants to write snowball confessions as outlined above.

All six pilot participants responded to all three prompts, giving instructors eighteen individual free-text comments. Although the sample size was small, trends emerged within the responses. Four comments expressed concern surrounding location services on apps and smart devices, along with a desire to assess these permissions more critically in the future. Three comments addressed the practice of storing passwords in browsers and the conviction to discontinue the habit of prioritizing convenience moving forward. Others generally expressed a commitment to being more vigilant in their auditing of online accounts, social media posts, and digital activity in the future. One comment that particularly stood out to the authors based on their philosophical approach to privacy literacy was "Privacy is very important to maintain your identity." Feedback that will help in future iterations of the workshop includes participants' curiosity about government surveillance. This can either be intentionally integrated into the Digital Shred Workshop content or be the basis of additional workshops in the PSU Berks Privacy Workshop Series.

In adapting to virtual delivery in fall 2020, worksheets were converted to fillable PDFs, and informal assessment was modified from the kinesthetic snowball confessions to an anonymous webform. Eighteen students attended the virtual Digital Shred Workshop at PSU Berks, ten of whom responded to all three of the optional prompts, providing thirty free-text comments. Similar to the in-person pilot workshop, the responses focused mainly on concerns relating to digital footprints, deletion of zombie accounts, and password security. Other general trends in the feedback were related to data breaches, comprehension of terms and conditions, technology addiction, and digital wellness concerns, as well as expressed commitments to make digital shred techniques a habit. One student expressed an interest in learning more about VPNs, specifically the instructors' recommendations relating to their use and effectiveness; this is certainly valuable feedback for future iterations of the workshop. Anecdotally, awareness of and discussions surrounding VPNs have increased in prevalence throughout the last year during the Privacy Workshop at PSU Berks, which suggests that highlighting this topic would be of interest.

The Digital Shred Workshop was first implemented at UF in fall 2020 with nineteen in attendance, and a second offering in spring 2021 saw seven in attendance. Participants in these workshops were a mix of students, faculty, and staff, differentiating them from the solely student audience of PSU Berks. Similar themes emerged from the formative assessment at UF. The majority of comments were related to zombie accounts and password security; additional feedback related to smart home devices, social media accounts, and browser privacy settings. Most responses expressed commitments to altering behaviors or practices to reflect espoused privacy values.

Overall, the comments suggested that participants departed feeling that the workshop had delivered on its promised learning outcomes. Participants not only left with a framework to assess their current online practices and tools to shred their digital activities, but with a new understanding of the value of privacy to individual identity.

Findings

This qualitative, evaluative case study of the Digital Shred Workshop examines academic librarians' response to Hagendorff's four problems with privacy literacy, including the integration of theory into learning activities, as well as participant engagement with learning activities and generalizable lessons learned to inform privacy literacy efforts in academic libraries. Workshop developers aim to reduce barriers to access and use their privacy literacy learning experiences by licensing the learning activities, lesson plan, and privacy literacy toolkit as open educational resources (OER), promoting greater access to privacy literacy learning opportunities across demographic differences. By considering privacy in the past, workshop facilitators acknowledge that participants' privacy interests and concerns may shift over time, and that even the limited scope of rational privacy decisions that users are able to make can be the source of future privacy regrets. Digital shred tools and techniques are demonstrated to enable participants to remediate potential damage from the consciously given data of their past. Furthermore, introducing the concepts of behavioral surplus and data doubles reveals how numerous privacy challenges are beyond the direct, rational control of the user. Discussion of relevant privacy theories expands the focus of the workshop from the limited power of front-end privacy features. The original conceptual framework for Digital Shred, as depicted in figure 1, integrates concepts and techniques from a range of disciplines, including business, data science, and intelligence tradecraft, to develop a theory-informed privacy literacy learning experience. Applying concepts from risk management, storage efficiency, and data governance, including behavioral surplus and data doubles, allows workshop facilitators to place front-end privacy literacy tools and behaviors in a broader theoretical context. Furthermore, introducing the concepts of behavioral surplus and data doubles challenges responsibilization by revealing the range of data collection and data brokerage practices that are beyond the control of the user, and which may only be redressed by voluntary private sector action or state regulation.

Workshop facilitators evaluated participant engagement in learning activities through peer observation, instructor self-reflection, and analysis of participant responses to formative assessment questions. Peer observation and instructor self-reflection confirm that participants are actively engaged in the fact or fiction prior knowledge assessment, learning activity worksheets, large group discussion of the ideal portfolio activity, and the large group data integrity activity Have I Been Pwned? Analysis of participant responses to formative assessment questions reveal that participants value information about a wide range of privacy topics, including account security, wellness and technology, mobile and smart home devices, VPN services, location services and settings, and strategies for generally reducing their digital footprints. Numerous participants expressed an explicit commitment to actively manage their digital dossier. These findings suggest that workshop facilitators successfully engaged participants in activities to achieve workshop learning outcomes.

Through this qualitative evaluation of a novel privacy literacy learning experience, the authors identified conditions for success and other lessons learned that may benefit other academic librarians undertaking similar efforts. These generalizable findings include learning design considerations, leveraging OERs, and forming collaborative efforts, and are discussed in more detail below.

Limitations

The qualitative case study method presents limitations. First, case studies examine a "sample of one"[48]—in this case, a single privacy literacy workshop—and the qualitative methods of document analysis, observation, and free-response feedback are not readily scalable. The specific findings from a single evaluative case study might not be generalizable to other cases, although some general principles of privacy literacy learning design are transferrable to other teaching contexts. Second, the total number of workshop participants opting-in to provide feedback was small, at forty two (sixteen at PSU Berks and twenty-six at UF). While clear trends emerged in this qualitative feedback data, it cannot be assumed to represent the interests and experiences of all participants. Third, the personal involvement of the authors in developing, delivering, and evaluating the workshop under analysis introduces subjectivity and personal bias in the case study. In first-person qualitative studies, such subjectivity can be a source of analytical insight when bias is regulated by methodological rigor, including using multiple modes of analysis (such as document analysis, observation, and participant feedback grounded in a theoretical framework).[49]

Future Directions

This qualitative, evaluative case study considers implications for privacy literacy programming, provides insights for success, and suggests future directions for privacy literacy efforts in academic libraries. Prior research reveals that academic librarians are interested in undertaking privacy literacy work but lack the time necessary to cultivate professional self-efficacy, develop privacy literacy learning activities, and deliver them in course-embedded instruction.[50] The Digital Shred Workshop collaboration experience is evidence that one can leverage the process of developing learning activities as an opportunity to simultaneously develop subject matter knowledge and teaching confidence. Furthermore, by developing hands-on learning activities that are exploratory and open-ended by design, the workshop facilitator can step out of the "sage on a stage" role and act as a "guide on the side," modeling intellectual humility, curiosity, and learning alongside students as they progress through the workshop activities.

This is not to deny the need for privacy literacy learning design tools and OER. PSU Berks coauthors' Digital Shred Privacy Literacy Toolkit quickly expanded beyond How-tos to become a resource to assist and strengthen development of privacy literacy initiatives and professional development outreach. The toolkit now offers a freely accessible, curated repository of privacy literacy-focused teaching materials, toolkits, case studies, current awareness resources, professional guidance documents, and research, and can be used to inform and inspire privacy literacy program development. In addition to incorporating existing resources, the use of real-world artifacts, such as privacy auditing frameworks or the US intelligence community's damage assessment protocol, also provide readily adaptable learning materials. The Digital Shred Privacy Literacy Toolkit is designed to save the time of librarians who are delivering privacy literacy programs, so that they can focus on the pedagogical aspects of articulating learning outcomes, crafting engaging learning experiences, designing accessible and inclusive learning activities, and establishing curricular and co-curricular partnerships. Curating existing resources is also an intentional strategy to develop privacy literacy instruction resources that are sustainable over the long term.

Librarians who develop successful privacy literacy instructional materials are further encouraged to deposit them in an OER repository, such as the ACRL Sandbox or Loyola Marymount University Library's Project CORA,[51] and to share them through professional and scholarly communication. Sharing successful privacy literacy programming materials is another tactic to overcome the obstacles of lack of time and resources to develop content; and, as demonstrated in this case study, participating in privacy literacy scholarly communication and professional development will help expand the network of subject matter experts and practitioners.

A factor that contributed significantly to the success of the Digital Shred Workshop, and which is readily replicable, is that it developed through collaboration. Collaborative learning design introduces new perspectives and insights into workshop content, while many hands make light work of the task of developing learning materials, and collaborators are an invaluable source of peer feedback on instruction. Adaptive, technology-mediated teaching and learning modalities, which normalized in response to the pandemic, have made intra- and inter-institutional collaboration increasingly possible. Librarians are encouraged to seek privacy literacy programming partners, which can include co-curricular opportunities, within their institutions and professional networks.

It is crucial to acknowledge that discussion of ubiquitous privacy intrusions, surveillance, disparate harms, and what often amounts to unregulated social engineering can lead to a sense of helplessness, despair, or nihilism in students and librarians alike. Library instructors should coach students both to identify, and acknowledge the limitations of, their locus of control with respect to privacy issues, with due consideration for information asymmetries and the control paradox.[52] As an emerging area of instruction, privacy literacy lends itself to creative instructional approaches and hands-on learning activities. Gamification (such as the trivia-based prior knowledge check and character development Ideal Portfolio exercise), tongue-in-cheek humor (such as the activity prompts for the Ideal Portfolio and Damage Assessment exercises), speculative storytelling, and satire offer avenues to explore privacy issues while sustaining creativity, resilience, and well-being.[53]

Conclusion

This qualitative, evaluative case study presents the conceptual framing, institutional context, workshop learning experience, and participant response to the Digital Shred Workshop, with considerations for the future direction of privacy literacy programming in academic libraries.

It considers conditions for success, including collaboration, resources for developing knowledge and self-efficacy, backward design and student-centered learning design, adaptation of real-world artifacts, gamification, and theory-informed practice. Privacy literacy instruction and programming is an emerging area of academic library practice that applies core library values and expertise to a burgeoning social problem that people increasingly care about. Librarians are encouraged to explore the varied possibilities of privacy literacy programming in their disciplinary and institutional contexts.

Appendix A

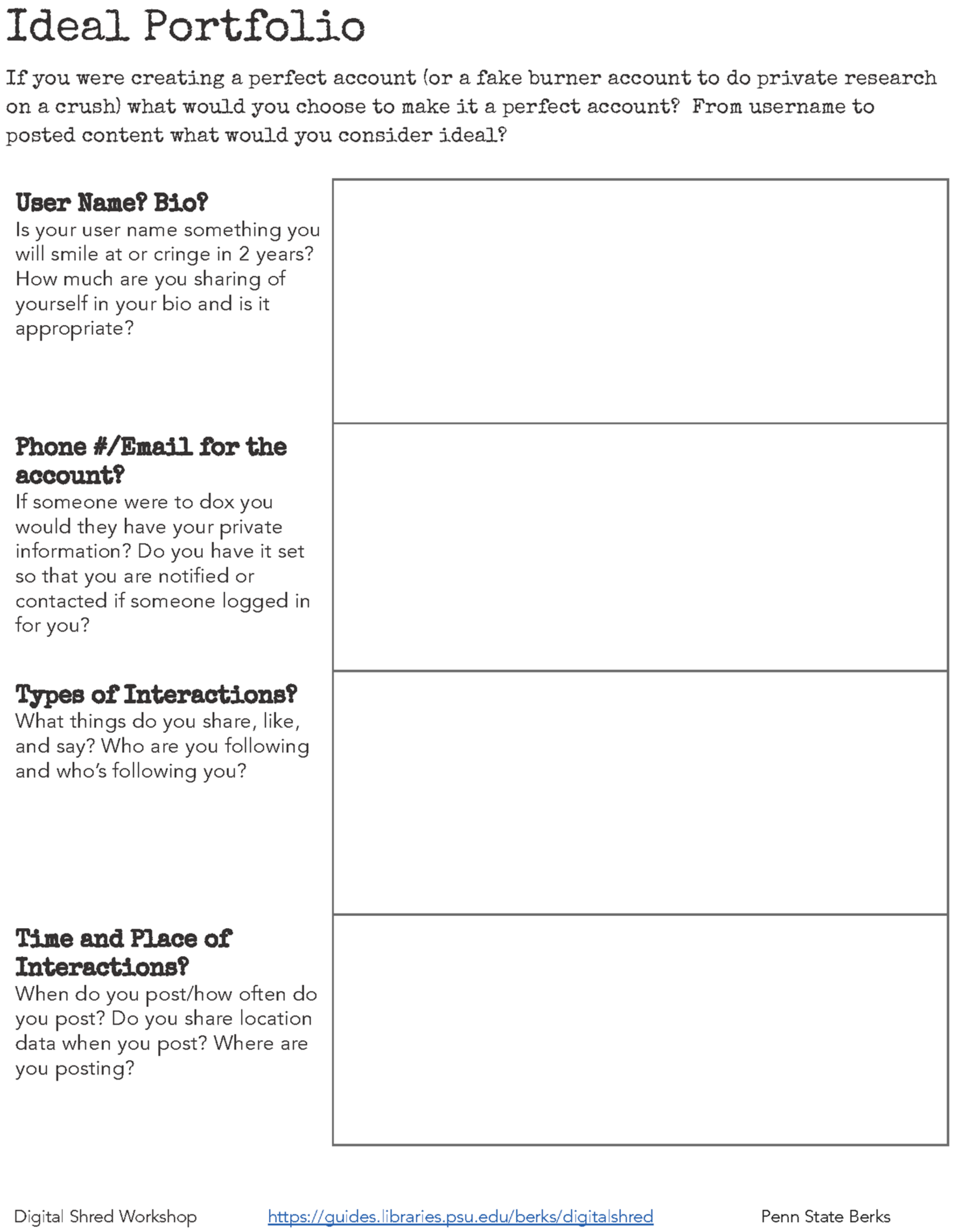
Gamified Prior Knowledge Check (Kahoot Quiz)

Includes the following ‘Fact or Fiction’ statements:

1. Using incognito mode in my web browser makes me invisible online.
   a. Answer: fiction
2. If I am not logged into any social media accounts, I am anonymous online.
   a. Answer: fiction
3. Websites are tracking my location, what I do, how long I am browsing, when I return, & much more.
   a. Answer: fact
4. Facebook tracks your online behaviors across the entire web, not just on their site.
   a. Answer: fact
5. Google search results are personalized based on your browsing history & online behaviors.
   a. Answer: fact
6. My online search history / activity is private.
   a. Answer: fiction
7. My social media activity will not impact my education or career because I have my accounts set to private.
   a. Answer: fiction
8. Websites / social media sites only use my data for targeted advertising.
   a. Answer: fiction

***Tip: As you move through the quiz it is helpful to give a brief explanation / context as to why each statement is fact or fiction.*

Appendix B



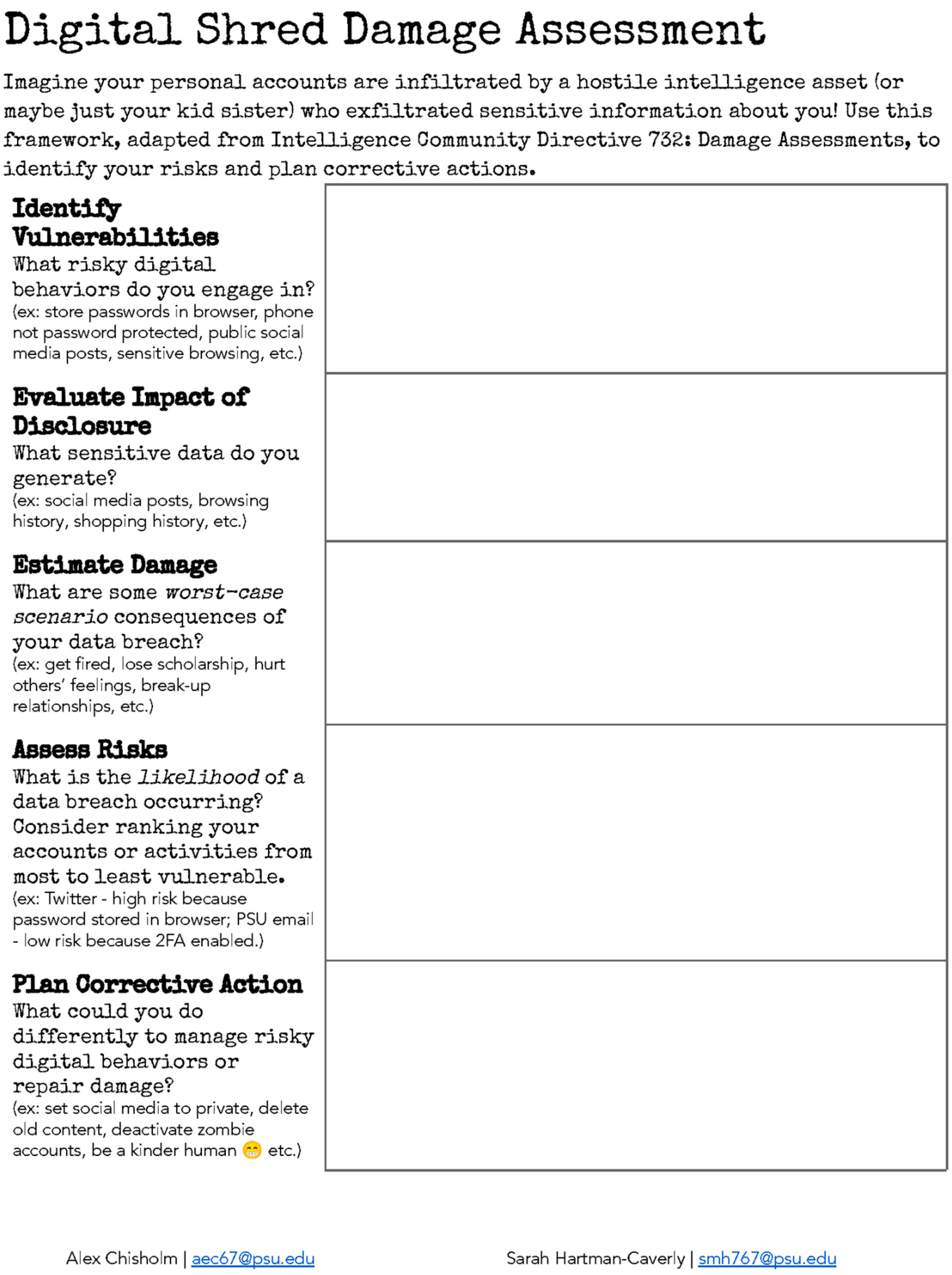
Ideal Portfolio

If you were creating a perfect account (or a fake burner account to do private research on a crush) what would you choose to make it a perfect account? From username to posted content what would you consider ideal?

User Name? Bio? Is your user name something you will smile at or cringe in 2 years? How much are you sharing of yourself in your bio and is it appropriate?	
Phone #/Email for the account? If someone were to dox you would they have your private information? Do you have it set so that you are notified or contacted if someone logged in for you?	
Types of Interactions? What things do you share, like, and say? Who are you following and who's following you?	
Time and Place of Interactions? When do you post/how often do you post? Do you share location data when you post? Where are you posting?	

Digital Shred Workshop https://guides.libraries.psu.edu/berks/digitalshred Penn State Berks

Appendix C



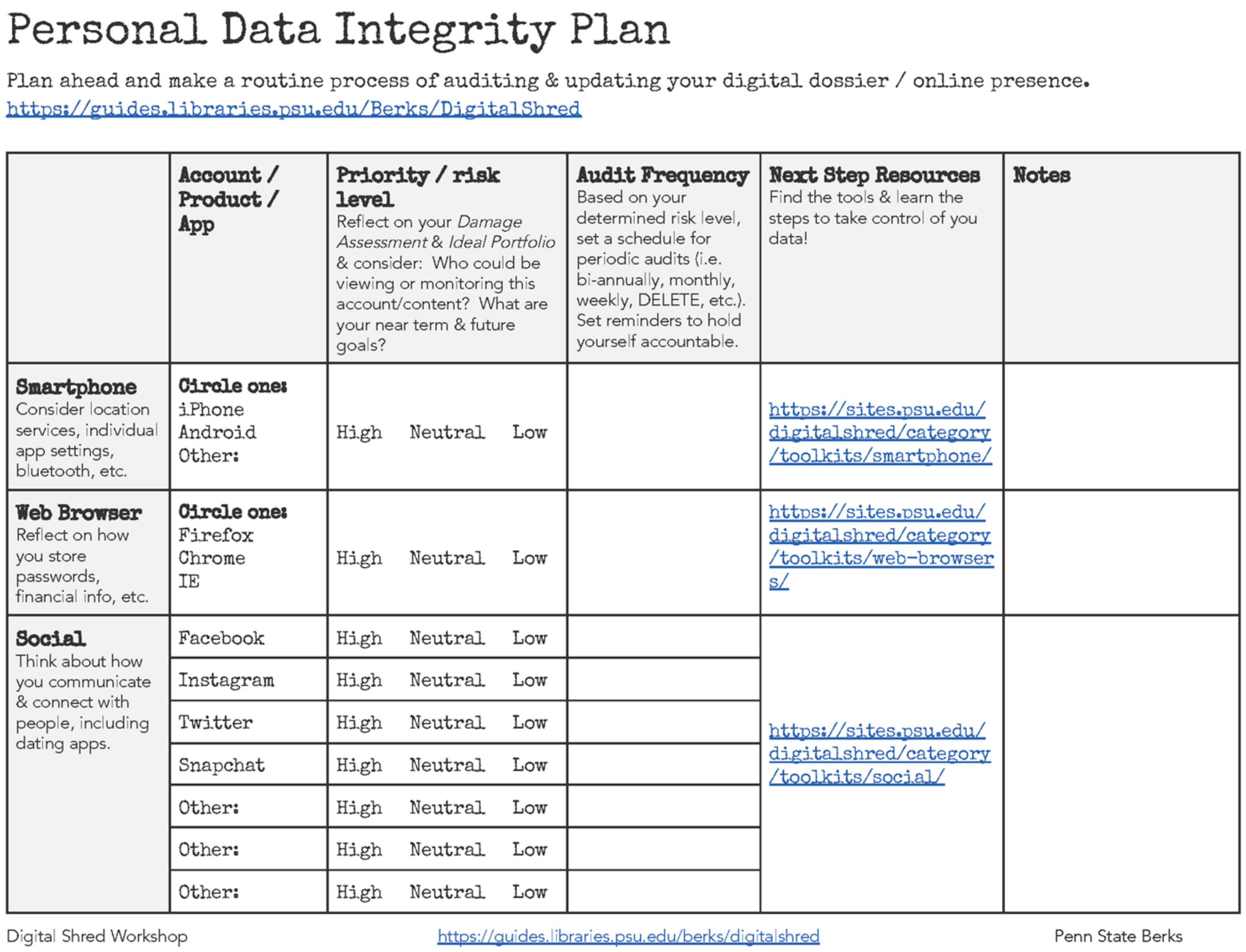
Digital Shred Damage Assessment

Imagine your personal accounts are infiltrated by a hostile intelligence asset (or maybe just your kid sister) who exfiltrated sensitive information about you! Use this framework, adapted from Intelligence Community Directive 732: Damage Assessments, to identify your risks and plan corrective actions.

Identify Vulnerabilities What risky digital behaviors do you engage in? (ex: store passwords in browser, phone not password protected, public social media posts, sensitive browsing, etc.)	
Evaluate Impact of Disclosure What sensitive data do you generate? (ex: social media posts, browsing history, shopping history, etc.)	
Estimate Damage What are some *worst-case scenario* consequences of your data breach? (ex: get fired, lose scholarship, hurt others' feelings, break-up relationships, etc.)	
Assess Risks What is the *likelihood* of a data breach occurring? Consider ranking your accounts or activities from most to least vulnerable. (ex: Twitter - high risk because password stored in browser; PSU email - low risk because 2FA enabled.)	
Plan Corrective Action What could you do differently to manage risky digital behaviors or repair damage? (ex: set social media to private, delete old content, deactivate zombie accounts, be a kinder human 😁 etc.)	

Alex Chisholm | aec67@psu.edu Sarah Hartman-Caverly | smh767@psu.edu

Appendix D

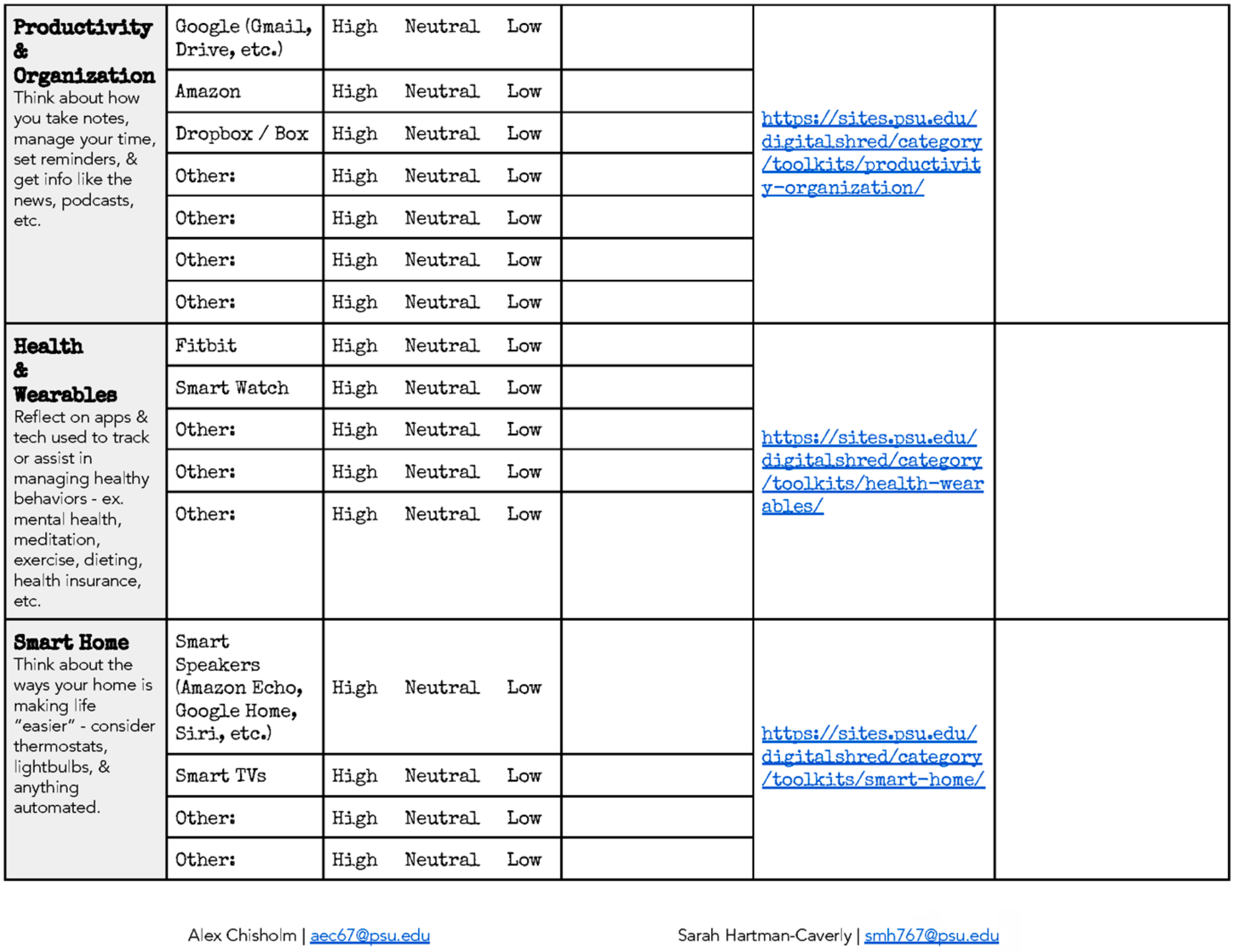


Personal Data Integrity Plan

Plan ahead and make a routine process of auditing & updating your digital dossier / online presence.
https://guides.libraries.psu.edu/Berks/DigitalShred

	Account / Product / App	**Priority / risk level** Reflect on your *Damage Assessment* & *Ideal Portfolio* & consider: Who could be viewing or monitoring this account/content? What are your near term & future goals?	**Audit Frequency** Based on your determined risk level, set a schedule for periodic audits (i.e. bi-annually, monthly, weekly, DELETE, etc.). Set reminders to hold yourself accountable.	**Next Step Resources** Find the tools & learn the steps to take control of you data!	**Notes**
Smartphone Consider location services, individual app settings, bluetooth, etc.	**Circle one:** iPhone Android Other:	High Neutral Low		https://sites.psu.edu/digitalshred/category/toolkits/smartphone/	
Web Browser Reflect on how you store passwords, financial info, etc.	**Circle one:** Firefox Chrome IE	High Neutral Low		https://sites.psu.edu/digitalshred/category/toolkits/web-browsers/	
Social Think about how you communicate & connect with people, including dating apps.	Facebook	High Neutral Low		https://sites.psu.edu/digitalshred/category/toolkits/social/	
	Instagram	High Neutral Low			
	Twitter	High Neutral Low			
	Snapchat	High Neutral Low			
	Other:	High Neutral Low			
	Other:	High Neutral Low			
	Other:	High Neutral Low			

Digital Shred Workshop https://guides.libraries.psu.edu/berks/digitalshred Penn State Berks



Productivity & Organization Think about how you take notes, manage your time, set reminders, & get info like the news, podcasts, etc.	Google (Gmail, Drive, etc.)	High Neutral Low		https://sites.psu.edu/digitalshred/category/toolkits/productivity-organization/	
	Amazon	High Neutral Low			
	Dropbox / Box	High Neutral Low			
	Other:	High Neutral Low			
	Other:	High Neutral Low			
	Other:	High Neutral Low			
	Other:	High Neutral Low			
Health & Wearables Reflect on apps & tech used to track or assist in managing healthy behaviors - ex. mental health, meditation, exercise, dieting, health insurance, etc.	Fitbit	High Neutral Low		https://sites.psu.edu/digitalshred/category/toolkits/health-wearables/	
	Smart Watch	High Neutral Low			
	Other:	High Neutral Low			
	Other:	High Neutral Low			
	Other:	High Neutral Low			
Smart Home Think about the ways your home is making life "easier" - consider thermostats, lightbulbs, & anything automated.	Smart Speakers (Amazon Echo, Google Home, Siri, etc.)	High Neutral Low		https://sites.psu.edu/digitalshred/category/toolkits/smart-home/	
	Smart TVs	High Neutral Low			
	Other:	High Neutral Low			
	Other:	High Neutral Low			

Alex Chisholm | aec67@psu.edu Sarah Hartman-Caverly | smh767@psu.edu

Notes

1. Sarah Hartman-Caverly and Alexandria Chisholm, "Privacy Literacy Instruction Practices in Academic Libraries: Past, Present, and Possibilities," *IFLA Journal* 46, no. 4 (December 2020): 306, https://www.doi.org/10.1177/0340035220956804.

2. Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, "Americans and Privacy: Concerned, Confused, and Feeling a Lack of Control over Their Personal Information," Pew Research Center, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/, accessed 10 June 2021.

3. American Civil Liberties Union, "Privacy and Technology," available at https://www.aclu.org/issues/privacy-technology, accessed 10 June 2021; Electronic Frontier Foundation, "Surveillance Self-defense," https://ssd.eff.org/, accessed 10 June 2021; Electronic Privacy Information Center, "EPIC Online Guide to Practical Privacy Tools," https://epic.org/privacy/tools.html, accessed 10 June 2021; Freedom of the Press Foundation, "Guide & Training," https://freedom.press/training/, accessed 10 June 2021.

4. Library Freedom, "Library Freedom Resources," https://libraryfreedom.org/resources/, accessed 10 June 2021; San Jose Public Library, "Virtual Privacy Lab," https://www.sjpl.org/privacy, accessed 10 June 2021.

5. American Library Association, "Library Bill of Rights," last modified January 29, 2019, http://www.ala.org/advocacy/intfreedom/librarybill, accessed 10 June 2021.

6. Association of College and Research Libraries, "Framework for Information Literacy for Higher Education," last modified January 11, 2016, http://www.ala.org/acrl/standards/ilframework, accessed 10 June 2021; ACRL Research and Planning Review Committee, "2021 Environmental Scan," last modified April 2021, http://www.ala.org/acrl/sites/ala.org.acrl/files/content/publications/whitepapers/EnvironmentalScan2021.pdf, accessed 10 June 2021.

7. Dana Rotman, "Are You Looking at Me?—Social Media and Privacy Literacy" (poster presentation, iConference, Chapel Hill, NC, February 8–11, 2009), http://hdl.handle.net/2142/15339, accessed 17 November 2021.

8. Rotman, "Are You Looking at Me?", 2.

9. Christina L. Wissinger, "Privacy Literacy: From Theory to Practice," *Communications in Information Literacy* 11, no. 2 (2017): 381, https://doi.org/10.15760/comminfolit.2017.11.2.9, accessed 17 November 2021.

10. Megan Lowe, "Information Literacy and Privacy/Security," *Codex: Journal of the Louisiana Chapter of ACRL*, no. 4 (2016)" 1–8, https://journal.acrlla.org/index.php/codex/article/view/123, accessed 17 November 2021; Eamon Tewell, "Toward the Resistant Reading of Information: Google, Resistant Spectatorship, and Critical Information Literacy," *portal: Libraries and the Academy* 16, no. 2 (2016): 306, https://doi.org/10.1353/pla.2016.0017, accessed 17 November 2021.

11. Lindsey Wharton, "Ethical Implications of Digital Tools and Emerging Roles for Academic Libraries, in *Applying Library Values to Emerging Technology: Decision-Making in the Age of Open Access, Maker Spaces, and The Ever-Changing Library*, ed. Peter D. Fernandez and Kelly Tilton (Chicago: ACRL), 45–47), http://purl.flvc.org/fsu/fd/FSU_libsubv1_scholarship_submission_1519756116_d2d8d648, accessed 17 November 2021.

12. Lauren Wittek, "Incorporating Online Privacy Skills into One-Shot Sessions," *Library Hi Tech News* 37, no. 4 (2020): 16.

13. Hartman-Caverly and Chisholm, "Privacy Literacy Instruction Practices in Academic Libraries," 312.

14. Alison J. Head, Barbara Fister, and Margy MacMillan, "Information Literacy in the Age of Algorithms: Student Experiences with News and Information, and the Need for Change," Project Information Literacy, last modified January 15, 2020, https://projectinfolit.org/pubs/algorithm-study/pil_algorithm-study_2020-01-15.pdf, accessed 17 November 2021, 14–16.

15. Thilo Hagendorff, "Privacy Literacy and Its Problems," *Journal of Information Ethics* 27, no. 2 (2018): 127–45.

16. Hagendorff, "Privacy Literacy and Its Problems," 130–33.

17. Hagendorff, "Privacy Literacy and Its Problems," 133–36; Head, Fister, and MacMillan, "Information Literacy in the Age of Algorithms," 14; Veronica Barassi, *Child | Data | Citizen: How Tech Companies Are Profiling Us from before Birth* (Cambridge: MIT Press, 2020), 34.

18. Hagendorff, "Privacy Literacy and Its Problems," 136–37; Chris Ip, "Who Controls Your Data?," *Engadget*, September 4, 2018, https://www.engadget.com/2018-09-04-who-controls-your-data.html, accessed 10 June 2021.

19. Hagendorff, "Privacy Literacy and Its Problems," 138–40.

20. Hartman-Caverly and Chisholm, "Privacy Literacy Instruction Practices in Academic Libraries," 306–8.

21. Sarah Hartman-Caverly and Alexandria Chisholm, "Transforming Privacy Literacy: From Surveillance Theory to Teaching Practice," (Conference presentation, LOEX, May 13, 2021), https://doi.org/10.26207/417p-p335, accessed 17 November 2021.

22. Helen Simons, "Case Study Research: In-depth Understanding in Context," in *The Oxford Handbook of Qualitative Research*, ed. Patricia Leavy (Oxford: Oxford University Press, 2014), 455–70.

23. Simons, "Case Study Research," 460–63.

24. "Berks Thun Library, Penn State Berks," last modified 2021, https://libraries.psu.edu/berks; "Penn State Berks at a Glance," last modified 2021, https://berks.psu.edu/penn-state/penn-state-berks-glance.

25. Alexandria Chisholm and Sarah Hartman-Caverly, "Privacy Workshop Series," last modified December 8, 2020, https://guides.libraries.psu.edu/berks/privacyseries.

26. Marston Science Library, "Science librarians," last modified 2021, https://marston.uflib.ufl.edu/about/science-librarians/; University of Florida, "About," http://www.ufl.edu/about/.

27. Emily Ford, "Consensus Decision-Making and Its Possibilities in Libraries," *In the Library with the Lead Pipe* (January 25, 2012), http://www.inthelibrarywiththeleadpipe.org/2012/consensus/, accessed 10 June 2021; Donna Harp Ziegenfuss and Sarah LeMire, "Backward Design: A Must-Have Library Instructional Design Strategy for Your Pedagogical and Teaching Toolbox," *Reference & User Services Quarterly* 59 no. 2 (2019): 107–12, https://doi.org/10.5860/rusq.59.2.7275.

28. Alexandria Chisholm, Sarah Hartman-Caverly, and Alexandrea Glenn, "Digital Shred Workshop," ACRL Framework for Information Literacy Sandbox, last modified in 2019, https://sandbox.acrl.org/library-collection/digital-shred-workshop.

29. John Doorley and Helio Fred Garcia, *Reputation Management* (New York: Routledge, 2020); Shuzhe Yang, Anabel Quan-Haase, Andrew D. Nevin and Yimin Chen, "The Role of Online Reputation Management, Trolling, and Personality Traits in the Crafting of the Virtual Self on Social Media," in *The SAGE Handbook of Social Media Research Methods*, ed. Luke Sloan and Anabel Quan-Haase (London: Sage, 2016), 74–89.

30. Rotman, "Are You Looking at Me?"; Wissinger, "Privacy Literacy: From Theory to Practice"; Lauren Wittek, "Incorporating Online Privacy Skills into One-Shot Sessions," *Library Hi Tech News* 37, no. 4 (2020): 15–17.

31. Thilo Hagendorff, "Privacy Literacy and Its Problems"; Laura Brandimarte, Alessandro Acquisti, and

George Loewenstein, "Misplaced Confidences: Privacy and the Control Paradox," *Sage Psychological and Personality Science* 4, no. 3 (2012): 340–47, https://doi.org/10.1177/1948550612455931.

32. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future on the New Frontier of Power* (New York: Hatchette, 2019), 80.

33. Jeffrey S. Shell, "Taking Control of the Panopticon: Privacy Considerations in the Design of Attentive User Interfaces" (Conference workshop presentation, CSCW Workshop, New Orleans, November 16, 2002), https://smg.media.mit.edu/cscw2002-privacy/submissions/jeff.pdf, accessed 10 June 2021; Alexandre Fortier and Jacquelyn Burkell, "Hidden Online Surveillance: What Librarians Should Know to Protect Their Own Privacy and That of Their Patrons," *Information Technology and Libraries* 34, no. 3 (2015): 59–72, https://www.doi.org/10.6017/ital.v34i3.5495; C. Ip, "Who Controls Your Data?"

34. Solon Barocas and Andrew D. Selbst, "Big Data's Disparate Impact," *California Law Review* 104, no. 3 (2016): 671–732, http://dx.doi.org/10.15779/Z38BG31; Ruha Benjamin, *Race after Technology: Abolitionist Tools for the New Jim Code* (Cambridge: Polity, 2019).

35. Evren Eryurek, Uri Gilad, Valliappa Lakshmanan, Anita Kibunguchy-Grant, and Jessi Ashdown, *Data Governance: The Definitive Guide* (Sebastopol: O'Reilly, 2021).

36. National Counterintelligence and Security Center, "Damage Assessments," https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-damage-assessments-mission, accessed 10 June 2021.

37. Hartman-Caverly and Chisholm, "Transforming Privacy Literacy."

38. Shell, "Taking Control of the Panopticon."

39. Barocas and Selbst, "Big Data's Disparate Impact"; Benjamin, *Race after Technology*; Ip, "Who Controls Your Data?"

40. Head, Fister, and MacMillan, "Information Literacy in the Age of Algorithms."

41. Office of the Director of National Intelligence of the United States of America, "Intelligence Community Directive 732: Damage Assessments," last modified January 27, 2014, https://www.dni.gov/files/documents/ICD/ICD%20732.pdf, accessed 10 June 2021.

42. American Library Association, "A Privacy Audit," Privacy Tool Kit, last modified January 2014, http://www.ala.org/advocacy/privacy/toolkit/policy#privacyaudit, accessed 10 June 2021.

43. Troy Hunt, "Have I Been Pwned?," https://haveibeenpwned.com/, accessed 10 June 2021.

44. Surya Mattu, "Blacklight: A Real-time Website Privacy Inspector," The Markup, https://themarkup.org/blacklight, accessed 10 June 2021; "Create An Alert," Google Search Help, https://support.google.com/websearch/answer/4815696?hl=en, accessed 10 June 2021.

45. Alexandria Chisholm and Sarah Hartman-Caverly, Digital Shred Privacy Literacy Toolkit, last modified 2022, https://sites.psu.edu/digitalshred/.

46. Kayce Mobley and Sarah Fisher, "Ditching the Desks: Kinesthetic Learning in College Classrooms," *The Social Studies* 105, no. 6 (2014): 301–9, https://doi.org/10.1080/00377996.2014.951471.

47. Mary J. Snyder Broussard, "Using Games to Make Formative Assessment Fun in the Academic Library," *The Journal of Academic Librarianship* 40, no. 1 (2014): 35-42, https://doi.org/10.1016/j.acalib.2012.12.001.

48. Simons, "Case Study Research," 458.

49. Simons, "Case Study Research," 459.

50. Hartman-Caverly and Chisholm, "Privacy Literacy Instruction Practices," 314.

51. Association of College and Research Libraries, ACRL Framework for Information Literacy Sandbox, https://sandbox.acrl.org/, accessed 10 June 2021; Loyola Marymount University Library, Community of Online Research Assignments, https://www.projectcora.org/, accessed 10 June 2021.

52. Geoffrey Lightfoot and Tomasz Piotr Wisniewski, "Information Asymmetry and Power in a Surveillance Society," *Information and Organization* 24, no. 4 (2014): 214–35, https://doi.org/10.1016/j.infoandorg.2014.09.001; Brandimarte, Acquisti, and Loewenstein, "Misplaced Confidences."

53. Sarah Hartman-Caverly and Alexandria Chisholm, "Ok, Doomer: Privacy Instruction Strategies to Lighten the Mood—and Your Workload" (Lightning talk, Penn State University Libraries Instruction Community of Practice, Spring 2021 Workshop), https://doi.org/10.26207/5mq6-1y46; Jen Ross, "Telling Data stories," Co-designing with Speculative Data Stories: Higher Education after Surveillance, last modified 2021, http://datastories.de.ed.ac.uk/, accessed 10 June 2021; The Light Phone, Introducing the Smartphone™, available online at https://the-lightphone.squarespace.com/smartphonetm, accessed 10 June 2021.