Article

Current Sociology
1–18

DOI: 10.1177/00113921221111819
journals.sagepub.com/home/csi
SAGE

Digital home-lessness: Exploring the links between public Internet access, technological capital, and social inequality

Matt Comi, Sarah Smith, Walter A Goettlich, Perry Alexander, Drew Davidson and William G Staples
The University of Kansas, USA

Abstract
Millions of individuals in the United States without a computer or broadband at their residence must rely on public libraries for their Internet access. Drawing on a rich data set of interviews and participant observation at three public libraries, we explore how individuals navigate these complex settings and how they profoundly shape their digital lives and experiences, one we characterize as *digital home-lessness*. In this article, we identify three themes that characterize the relationship between library computer use and digital home-lessness: *lifeline* encompasses the diverse set of activities that require computer and broadband access; *negotiating access* focuses on usability, privacy, and security disadvantages among these users; and *risky business* concentrates on the multiplicities of insecure Internet and computing practices exacerbated by low technological capital. Our findings push forward literature on the digital divide by illuminating how the experience of digital home-lessness limits social inclusion and reproduces socioeconomic inequality.

Keywords
Digital divide, inequality, Internet access, technological capital, surveillance

Introduction
As government agencies, education providers, employers, hospitals and medical offices, news and social media, polling organizations, and knowledge producers have moved

Corresponding author:
Matt Comi, The University of Kansas, Fraser Hall 713, 1415 Jayhawk Blvd, Lawrence, KS 66045, USA.
Email: mcomi@ku.edu

online, ready access to broadband Internet has become a 'basic requirement for social and economic inclusion' (Dailey et al., 2010: 4). Despite improvements in broadband infrastructure, profound and persistent disparities in Internet access continue, resulting in a 'digital divide'. This is exacerbated by the slowed development of broadband service expansion. The number of American adults with broadband service at home increased rapidly in the early 21st century; however, progress in adoption has since been 'much more sporadic' and has now fallen off from a high of 73% in 2016 to 65% in 2018 (Pew Research Center, 2018). About 2% still use slow dial-up connections and the rest live in effectively disconnected households. Disparities in broadband access continue to reflect the familiar patterns of socioeconomic inequality: 9 out of 10 college graduates have broadband at home compared with just 34% of those who have not completed high school; adults under age 50 are more likely than older adults to have Internet access at home; 78% of European Americans have access to high-speed Internet, while 65% of African Americans and only 58% of Latinx individuals do; those living in households earning at least US$50,000 per year are far more likely to have home broadband than those at lower income levels; and those living in rural areas are as much as 12% behind those in cities and suburbs (Pew Research Center, 2018; U.S. Council of Economic Advisers, 2016).

For this project, we conducted ethnographic observations and 40 in-depth interviews with patrons and staff of public libraries in two diverse communities in the US Midwest. From these data, we have generated detailed and nuanced knowledge of library patrons' day-to-day successes and challenges, security and privacy experiences and concerns, and their technical needs and skill requirements as they navigate these social and digital spaces. Lacking a secure digital 'home' or robust digital resources in their communities, our computer users have unusually low technological capital (Carlson and Isaacs, 2018). However, rather than simply existing on the low end of a spectrum of skills, these individuals' experiences are the result of a categorically different relationship to the Internet and computer resources, one we characterize as 'digital home-lessness'. In this article, we illuminate three aspects of the lived experience of digital home-lessness: *lifeline* encompasses the diverse set of activities that require computer and broadband access; *negotiating access* focuses on usability, privacy, and security disadvantages among these users; and *risky business* concentrates on the multiplicities of insecure Internet and computing practices exacerbated by low technological capital. Our analysis demonstrates a more nuanced view of the digital divide, to better capture, study, and eventually remediate the socioeconomic disadvantages of this population. Our empirical work within these library systems has relevance throughout the United States and elsewhere in the globe where unequal access to broadband infrastructure remains pervasive. Theoretical implications from our findings advance the sociological discourses on the digital divide, inequality, and social inclusion in an era marked by unequal access to digital resources.

Background: inequality, access, and public libraries

Digital inequality

Access, inclusion, and technological innovation (re)produce a range of social and economic inequalities (Roth and Luczak-Roesch, 2020). Surveilled spaces (Foucault, 1977;

Staples, 2014), along with the quickly changing texture of web-based data collection and its uses (Fuchs, 2013; Prince, 2018; Smith, 2017), result in varied yet widespread experiences of digital/social inequality (Halford and Savage, 2010; Madianou, 2015). While some study surveillance as the social force which produces unequal outcomes (Ajunwa et al., 2016; Gangadharan, 2013), others have focused on the implications arising from particular technical arrangements that allow for future Internet surveillance (Baek, 2014). Our research keeps both surveilling entities and technical arrangements in mind. However, we additionally consider the *physical spaces* in which these social practices take place for our target population – keeping in mind that the material experiences of computer users extend beyond distinctly digital spaces.

Marginalized Internet users may be more likely targets of online scams, identity theft, differential pricing of goods, and discriminatory profiling when they do go online (Andrejevic, 2014; Gangadharan, 2013; Gumbus and Grodzinsky, 2015; Hannak et al., 2014; Madden, 2017; Newman, 2014; Ohm, 2010). And while almost all Internet users are 'sorted' into a variety of social, economic, and cultural categories (Barocas and Selbst, 2016; Edelman and Luca, 2014; Gandy, 1993; Gumbus and Grodzinsky, 2015; Lyon, 2003; Madden et al., 2017), our target population of public computer users may be even more vulnerable. The direct impact of such experiences on the precarious lives of many public computer users can be profound; scams and sorting may reduce already limited financial means, affect employment opportunities, undermine credit worthiness, limit access to suitable housing, and threaten the provision of much needed governmental support and services (Bruckner, 2018; Narayanan, 2011; Newman, 2014; Nissenbaum, 2010; Selwyn, 2004). Digital discrimination and online victimization experiences may prompt marginalized Internet users to self-restrict their online activity, further exacerbating their social and civic isolation, reinforcing preexisting inequalities, and channeling life chances downward (Fisher, 2009; Gangadharan, 2017; Hannak et al., 2014; Madden, 2017; Pasquale, 2015).

Our study responds to a growing concern that there remains a lack of solutions-oriented engagements for remediating the material experiences of public computer users impacted by the widening *digital divide* (Crawford, 2014). The term *digital divide* addresses the problem of inequalities in digital spaces, often glossed as problems of literacy and access, which may be better thought of as inequalities in *technological capital* (Carlson and Isaacs, 2018). In Carlson and Isaac's (2018) alternative to *digital divide* thinking, *technological capital* is a measure of accrued history with information and computers technologies as assessed through 'awareness, knowledge, access, and technological capacity of the user's social collective' (p. 243). Drawing on this approach, we emphasized two components of technological capital: access and technological capacity – being broadly concerned with how the material contexts of our population informed experiences of inequality and (in)security when using public-access computers. What we find is that public access and limited capacity are further exacerbated by our many users who do not have a secure 'digital home'.

Digital access and public libraries

US households with broadband and computers have a distinct set of social, economic, and technological advantages that are derived from having a 'digital home'. Residential broadband and computer ownership offers convenient and unlimited use of online platforms

including low-cost online education; private access to medical care and medical information; a key source of news, politics, community engagement, and support for entrepreneurship and small businesses; and critical tool for seeking and maintaining employment opportunities. Moreover, users have control over the installation of software they chose to use, the format and organization of folder systems, and convenient access to large data and documents storage, and they have control over their security and privacy settings on their computers and network/routers.

In contrast, the computing lives of those without digital homes are resource-limited, less private, less secure, and more transient than those who own their computers and have convenient broadband access. Because of the circumstances faced by public library Internet users in the US Midwest − where limited mass transit, sprawling suburban spaces, and rural distances make access to public Internet resources that much more challenging − we have found those without personal computer hardware face unique, complex, and intersecting challenges that compound those typically associated with digital inequality. This access divide is a core policy concern in the United States, and the inequality in access correlates with existent inequalities, with lower earning and lower educated individuals being the least likely to have a secure digital home, while having a digital home is nearly a given among higher earning or higher-educated individuals (US Council of Economic Advisers, 2016). However, much of the research on this issue ignores material aspects experienced by individuals obligated to use public services, such as those offered by libraries to achieve core social functions available on digital platforms.

We have come to characterize these experiences as *digital home-lessness*. With every visit, these users start new sessions on library system computers that do not permit users to save their files, website bookmarks, or passwords or modify functional preferences or privacy and security settings. Most users are left with the burden of starting from scratch each session and have no choice but to use to the privacy and usability defaults set by the library. Not only does this make for a limited computing experience, but it may leave them more vulnerable to security threats and privacy violations. Computer users, especially public computer users, face a range of differential online treatments that compound issues of security and privacy, increasing overall affinity for high-risk digital behaviors. Library computer labs provide a range of services which give access to both Internet and basic computer workstation functions (Becker et al., 2010). While libraries have generally shifted their services to better supply functioning workstations and tech services, they have struggled to mitigate these risks and provide holistically accessible computer resources to the full socioeconomic range of library patrons (Bertot et al., 2012; Crawford, 2014). Put differently, libraries deploy a range of digital support features (firewalls, preloaded desktop shortcuts) and material infrastructures (support staff, privacy partitions, signage) but continue to witness risky computer behaviors and difficulty completing users' goal tasks.

While those experiencing digital home-lessness may have email accounts or social media profiles, their ability to access their digital identity is resource-limited to public hardware. Their digital health and welfare are both fragile and vulnerable to intrusion and attacks, and individuals they are obliged to share these resources in close spatial proximity to others where screens can be 'shoulder-surfed' and where personal documents sent to communal printers are easily read or swiped. Unable to personalize their

temporary computing 'home', they must bring their digital lives along with them, stored on USB drives, hardcopy papers, passwords written in notebooks, or other analog solutions because they have no personal digital storage at the library and no home-based computer system.

Our findings show that the experiences faced by those lacking secure personal computer hardware are in a way that is often missed in discourses on digital inequality. The experience of digital home-lessness is not simply a condition on one end of a spectrum (e.g. low technological capital or low digital literacy) but rather a unique and complex situation that requires holistic study and policy amelioration. Remediating these users' awareness or knowledge through literacy courses or outreach helps to solve aspects of technological capital inequities, but it fails to capture the material inequalities caused by limitations in material access and capacity. We do not wish to draw a simplistic metaphor with those experiencing physical homelessness, who also face a variety of different intersecting inequalities. Rather, we wish to call attention to the distinctly material circumstances faced by those without a digital home which are often missed in discourses on digital inequality and the digital divide. To highlight this fine-grained differentiation, we use the term digital *home-lessness* as opposed to simply *homelessness*. Our empirics suggest that public Internet users' engagements with library computers are complex, distinctly material experiences that multiply the disadvantages faced by individuals experiencing other forms of inequality. Libraries may provide basic necessities and be an essential resource for these users – and most are deeply grateful for it – but it is not a substitute for the many functional, social, economic, and cultural benefits that are derived from having a secure computer and broadband at their residence.

Methods

Our qualitative and interpretive methods are designed to derive an in situ understanding of the everyday lives and activities of socially and economically marginalized individuals who may be difficult to locate through other methods (Lofland et al., 2006; Ragin et al., 2004; Warren and Karner, 2015). We sampled settings and participants for their ability to offer information about the lived experiences of library patrons who rely on public computers. Our goal is situational and logical generalizability rather than demographic or probabilistic representativeness as we aim to develop an explanatory theory that can be used to understand the experiences of those in comparable situations.

Data for this project were collected over a 10-month period from September 2017 to June 2018 and carried out in four library locations in two socially and economically diverse communities in the Midwest. Qualitatively trained researchers from our interdisciplinary team of social and computer scientists engaged in participant observation and conducted field interviews (Van Maanen, 2011). Field researchers volunteered as computer techs at library Help Desks, spending up to 15 hours per week in this role for approximately 700 total hours in the field. This proximity allowed the researchers to interact with and observe closely the patrons and staff in each setting and enabled them to observe the computer activities patrons engage in, the types of problems they encounter using computers and navigating the Internet, and the sorts of questions they have for support staff, especially those related to security and privacy such as inputting personal

data, the use of social media sites, creating passwords, and answering email from strangers. During this time, researchers collected fieldnotes which were coded and analyzed alongside our targeted interview data.

After a period of engagement in which the researchers established trust and rapport with participants, patrons who were regular public computer users were invited to participate in field interviews at the libraries and given US$25 cash in compensation for these interviews. During the interviews, patrons were asked both closed- and open-ended questions about their use of the Internet and their online privacy and security experiences. The researchers conducted 40 field interviews (33 patron, 7 staff) centered on patron use of library computers and their privacy and security experiences. Interview transcripts and fieldnotes were analyzed using the qualitative data analysis program *ATLAS.ti.* Interviews and fieldnotes were inductively coded, after which key codes were selected and the interviews were re-coded deductively according to these key codes (Bernard, 2011 [1940]). These codes form the basis for our broader three themes reported in the following results. All participants discussed in this article are referred to using pseudonyms.

Results

Our analysis describes the experience of digital home-lessness and how these experiences undermine the socioeconomic mobility and inclusion of library patrons through the usability, privacy, and security risks founded in public computer use. We present our empirics as in three primary themes. The first theme, *lifeline*, encompasses the diverse set of activities that require computer and broadband access, many of which are essential for socioeconomic mobility and participation in social life. The second theme, *negotiating access*, focuses on the unique opportunities and barriers experienced by public computer users that contribute to usability, privacy, and security disadvantages among the digitally home-less. The third theme, *risky business*, focuses on the multiplicities of insecure Internet and computing practices which are compounded by issues of literacy about safe and expedient computer use. The individuals experiencing digital home-lessness were particularly vulnerable to cyber-attacks and compromised privacy and, as a result, to cycles of inequality that disadvantage members of this population.

Lifeline

For a majority of the individuals we encountered, not having broadband and/or a computer at home was a function of limited income and economic resources. When considered in light of technological capital, these lifelines reveal the specific contours of life that higher technological capital enables. Our subsequent two themes (*negotiating access* and *risky business*) reveal specific pathways that limit these users' technological capital acquisition. This lack of technological capital is compounded in the intersecting experience of those without access to a stable home platform for computer use and Internet access – in other words, those experiencing digital home-lessness.

Many public computer users relied on library facilities to conduct important tasks related to their employment. These patrons carried out job searches, wrote job applications, and/or performed employment-related activities such as email correspondence,

accessing scheduling systems, and for a few, the management of small businesses they owned. Job applications often require not only broadband Internet access but also reliable, persistent Internet connections for time-intensive application processes and email communication. Our population of users experiencing digital home-lessness must conduct this personal business in a public setting. While our study could not examine the impact of this inequality on socioeconomic mobility, our observations suggest that there is a likely link between this experience of inequality and barriers to mobility long-term.

These issues and challenges were brought up frequently in our interviews with patrons. As Lois, a 62-year-old, long-time library user without home computer access, noted,

> I've been coming here at least three days a week . . . minimum. I always have to check my email to see if [company] is contacting me . . . The only way that they communicate with you is [through] email.

Even those with access to smartphones noted that many websites are inaccessible on mobile devices, and phones can be difficult to use for many purposes. One patron, John, told us, '[a smartphone is] a smaller screen and I'm typing everything by hand, so especially if I have a longer email, I prefer to have a keyboard'. Job applications often required resumes to be formatted using Microsoft Word, which presented another barrier to those without a computer at home or those who could not afford the software. One interviewee Hannah noted that

> usually the main reason that I would want to use the [library] computers is to use Microsoft Word, because I have a Chromebook at home, but the formatting isn't the same and when I'm doing job stuff, I like to use Microsoft Word because that's what companies use to look at stuff.

Job searches and applications are crucial for socioeconomic mobility and libraries provide essential access for some users to accomplish these tasks. However, using public platforms to complete online job applications, use job search sites, send emails, and write resumes often opens the user up to a higher level of risk, as compared to those with digital homes who can do them in private settings. Employment search and application documents and forms often require inputting a large amount of personally identifiable information that could expose public computer users to greater vulnerabilities compared to home computer users.

Many computer users who experience digital home-lessness also required computer and Internet access for financial activities, such as buying and selling items online, accessing pay stubs and online banking, filing taxes, checking credit reports, and applying for public benefits. For example, many patrons used library computers to buy or sell items on sites such as Craigslist, eBay, or Facebook Marketplace or to search for local giveaways and garage sales. One patron managed a small online shop, noting that on the website, 'I can't change credit card information and stuff on my phone, so that makes it pretty difficult to manage a website like that' (John). Some of the most financially disadvantaged patrons regularly used the library computers to make small amounts of money. For example, one physically homeless patron reported visiting

libraries most days (sometimes multiple libraries in a day due to computer use time limits) to complete online surveys for money, noting that the surveys could not be completed on a phone (Stanley). Other patrons used library computers for essential services, including filing their taxes or applying for benefits programs such as Supplemental Nutrition Assistance Program (SNAP), Lifeline Assistance (referred to as 'government phones'), Social Security, or managing VA benefits. One patron without home Internet access used library computers to 'stay aware of Medicare changes . . . which prescriptions are changing. I have to fight sometimes and advocate for myself' (Ruth). While these types of financial and public assistance activities are often critical for managing personal finances and wellbeing, these activities can expose important personal information when done in a public setting.

Others used public computers to advance their education or job training. These users reported a variety of essential work or education-related tasks, such as one nurse who relied on libraries for printing services: 'you have to be able to print off the completion certificate . . . so rather than risk losing the work on my phone, I'll go to the library to complete it all' (Olive). Other patrons used library computers to complete college or high school coursework. Although traditional high school students in the study communities now have access to laptops provided by their schools, many adult learners and those enrolled in college courses are required to locate their own computer and Internet access to complete coursework. This latter group uses library computers to research and write papers (which often requires Microsoft Word), attend on-line lectures, and deal with the administrative aspects of their education. For example, one participant experiencing physical homelessness reported using library computers daily to study for their GED and to apply for financial aid for college (Ryan).

Beyond the direct use of public-access computers to engage in education- or employment-related tasks, a majority of the public computer users also utilized the Internet for entertainment or social media access. These types of activities are an important component of personal wellbeing and social inclusion and may allow those experiencing digital home-lessness to maintain social networks and ties that could be utilized to increase technological capital. Jerry, a writer, expressed his experience of broadband Internet access in public libraries as 'a lifeline for me'. He went on to tell us:

> In a month, everything that I'm saying now could be completely different, 'cause I might not have a phone, I might not have a computer, and I might not have internet at all. [. . .] That would only work because I'd be in an environment where I've got two friends in the same house. They both have phones, they have Internet, which would make me feel like a mooch to some degree . . . But living alone, there's no way I would feel comfortable being completely cut off.

The precarity of Jerry's homelife and financial outlook demonstrates the importance of libraries as both physical spaces and places where computer and Internet access are made possible, if not ideal. Many patrons used library computers to access sites such as YouTube and Facebook for both entertainment and social networking. These engagements, which some might consider superfluous or *merely* entertainment, are nonetheless important aspects of these computer users' digital lives, and therefore a method by which computer use in library settings connects them to the social digital landscape.

The computer activities and needs described in this section demonstrate the importance of computer and broadband Internet access for mobility and inclusion as well as personal wellbeing. Safe, adequate, and accessible computer and Internet access has become an essential aspect of contemporary life and represents a critical mechanism in the (re)production of social inequality when these needs are not met. However, as we document below, many of these activities involve the use of personally identifiable information (PII) which can expose public computer users to differential privacy and security vulnerabilities and treatment compared to home users.

Negotiating access

Our findings primarily address issues of access and capacity – those factors of technological capital which are directly affected by the materiality of the computers and computer-using spaces provided by libraries. As we argue above, public-access computers do not provide the same socio-digital advantages as home broadband and a dedicated personal computer. Those requiring library computers are obliged to negotiate a host of access, usability, privacy, and security issues in these settings not typically experienced by those fortunate enough to compute from home. One simple limitation that compounds with other access concerns are time-limit policies designed to equitably share public computer resources. At one of the libraries we studied, the policy stated,

> All patrons are guaranteed 60 minutes without interruption the first time they sign in for computer use each day within the library's set hours for computer time. After the initial time period, the patron can be bumped to make room for a new user if there are no free computers. Once a patron has been bumped, he/she may sign on for computer use if one becomes open Patrons are allowed up to 3 hours of computer time per day, which may be lengthened at staff discretion.

One staff member, Harvey, told us,

> I think a lot of people wish it was a longer time limit, but we do have a lot of patrons that will stay at the library for 9 to 10 hours. So, if we allowed people to stay that long, we would not have enough computers for people just needing to come in for a little bit.

However, time limits can be problematic when people must complete long processes such as job applications, online training programs, and taxes.

Beyond personal inconvenience, this can result in rushed work and limited productivity. One interviewee said that they go to the library every day and use the entire time limit. This person also said 'it kills me' when the libraries close for a holiday or for staff events. Susan, an international university student on hiatus for the last year, noted that when she was taking classes, she would be at the library all day, every day. She explained that this was because

> [M]y typing speed is not good. My English – sometimes I make mistakes, so corrections, proofreading, everything, it will take a long time, so I come and make sure that I turn in and write everything just before the library closes. I rush and finish it up like that. Most of the week and Saturday I come here. But Sundays I don't come because there is not [public] transit.

Rules governing the library facilities and specifically the use of computers were another point of navigation for patrons to avoid losing privileges as was the authority of staff to apply policy as they saw fit – sometimes resulting in inconsistent enforcement of library rules.

In addition to these access challenges, public Internet users confront a unique set of usability hurdles. Experiencing digital home-lessness means that a patron's computing experience is highly transitory, and with every visit to the library patrons must begin with system-setting computers. At our research sites, as with many libraries, disk reimaging software was installed that would scrub all user data, website 'cookies', and entered information after the end of each session. A session ended either by the user logging out of the computer or it was automatically terminated after a short period of inactivity, typically 15 minutes. While this practice is intended to create a 'clean' workstation and safeguard user privacy by removing any personal information they may have left behind, it also meant that users lacked a digital home with persistent storage of files, the ability to save passwords and bookmark websites, or to set security and privacy preferences on Internet browsers. Therefore, configuration settings and security preferences on library computers must be reset with every session, a requirement that is inconvenient and time-consuming at best and, for many users, not likely undertaken without help from tech staff. In addition, even if they were savvy enough, at most libraries patrons were not able to install software on the machines. This limited their ability to work with specialized files, update an iPhone, or access certain learning sites.

Accessing the Internet in a public library was also less than ideal for many users because of fears that others could see what they were doing. The presence of others, especially strangers, limited access and usability as it hindered many from doing tasks that would make them feel vulnerable. None of our study locations' monitors were fitted with screen privacy filters, and at some sites there were no dividers between computers. Known as 'shoulder surfing', this activity may range from mild curiosity to a type of nefarious strategy used to obtain information such as personal identification numbers (PINs), passwords, and other confidential data. One patron, Peter, stated bluntly, 'if you don't mind broadcasting what you're looking at, go ahead and use [the community computer area], because people could walk around and look'. Another patron, Olive, said, 'I don't want anybody to look over my shoulder, so that makes me feel a little uncomfortable'. However, for many patrons, this risk was unavoidable when using library computers. Despite consistent concerns expresses by patrons, Edward, a staff member, suggested that surveillance by patrons was not usually an issue, and that 'generally when we see someone looking at someone else's computer, it's because that person is looking at something inappropriate'. Patrons are also vulnerable to privacy intrusions if they leave their computers unattended to go to the restroom, make a phone call, and the like.

Similarly, if a patron leaves the library and forgets to log off, the screen will remain active until it is automatically shut down. Another staff member, Larry, noted that

> people who don't have a library card will wait for that person who is unaware that they need to logout . . . and they will come right up after them, so that they can sneak in and get the rest of their time. At that point, I'm sure that [previous] person isn't logging out of things and has all their stuff open.

This person jumping on a session would not only have access to what was on the screen but also stored session data could reveal data such as login passwords, browsing histories, and personal files and information. On the other hand, users frequently found themselves automatically logged off from unattended computers. When this happened, if they had not saved their work to an external device, they lost everything they were working on. As one interviewee Roger, a 36-year-old salesman, said,

> This is really infuriating because it happened twice in three days: I was working on a pitch and stepped out to use the restroom, and while I was in the restroom [the computer] cycled off . . . I had spent like an hour and a half creating content, and then I asked the [staff member] if there was any way possibly to get it back, and she said 'no'.

While data loss can certainly occur with personal computer use, many programs offer auto recovery features, and there is greater control over system restarts. This kind of computer management and functionality is simply not available to public users.

Patrons had little choice but to accept many of these access and usability limitations or try to adapt to them with a variety of workarounds. They did their best to fit their schedules to those of the libraries. When some ran out of their allotted time, they would restart their use clock by visiting multiple libraries in a day. Users avoided 'shoulder surfing' by sitting, if possible, away from other patrons, rotating their computer screens, or completing their task as quickly as possible. Alternatively, without understanding how to lock screens using the reservations software, certain users would sit through marathon sessions to get the most use of their limited time as well as to avoid leaving their screens unprotected. Some brought their own USB flash drives or used smartphones to store files and passwords. However, these devices are rarely encrypted and created serious security and privacy risks if lost or stolen. Lost flash drives were not uncommon, and one patron said that 'when I was really working on two or three things at one time, just invariably I would always leave [my flash drive]'. Yet they noted that staff members knew them and would regularly collect unattended flash drives ([Linda). As a reminder, these USB drives are not useful for carrying data from public computers to home computers for individuals experiencing digital home-lessness. Rather, these thumb drives are the entirety of their digital home, and the data on them only translate into meaningful experiences in public computer settings.

Because of this, users face a variety of obstacles to the acquisition of digital literacy skills. Individuals with home computers have the opportunity to regularly practice digital skill development and to maintain access to important lines of communication for work and personal life. As an example of this obstacle, many of our users bring with them hardcopy lists of passwords or step-by-step instructions on how to use the computers or Internet. The inconsistencies across library systems and even between hardware within a library limit the effectiveness of these routinized instructions which often 'break' when a website is updated or when the library system is changed. Such 'breaks' prevent those experiencing this population from performing tasks they would otherwise have acquired the literacy to achieve. A number of patrons told us that they protected themselves from privacy violations by not engaging in activities requiring the input of personal information, but this strategy made the library facility less useful to them. Others turned to staff

whom they saw as trustworthy with their personal information, sometimes even asking staff to enter personal information for them. As one patron, Charlie, told us, 'Several guys down here [staff] have helped me out with, like, a job application, they see me enter the social or I would give that to them if I need to'.

Risky business

Our final theme, *risky business*, identifies and describes the way our research population faces barriers to safe Internet browsing because of the compounding inequalities that those without a secure digital home face. Particularly, we explore how these users lack the technological capital (Carlson and Isaacs, 2018) of digital literacy and Internet proficiency and suffer from a variety of security vulnerabilities. While library systems do feature design safeguards to remediate digital risks related to digital home-lessness, many of these same services face computer systems level and individual resistance. Many of our users face risks that are caused by problematic relationships with secure computer use in the physical space of a public library. One such behavior involves how users manage private information such as passwords. Linda, who is a middle-aged public-access library user who is currently unemployed, told us about her trouble with password management:

> Maybe because I have not handled computers. I am from a small island. I don't have that much exposure so I'm not always considering the dangers . . . I didn't know how to even handle email when I came in 2014. I studied it from [library staff member]. They have helped me. This library I will never forget . . . . I keep a small notebook and each password [and] I bring it to library in order to go to certain sites.

Many patrons like Linda memorized, reused, wrote down, and/or stored their passwords on a (likely unencrypted) mobile device, which often led to login difficulties. Those who memorized passwords often used short or simple passwords that were shared across multiple websites and accounts, rather than generating unique, randomized passwords. For example, Lois, who identified as a low-earning, self-employed, middle-aged woman, said, 'I've had the same [password] for 10 years and there's one variation . . . I know that that's not the thing to do but that's what I've done. I don't like to remember things'. In a public setting, passwords that are written or stored on a mobile device could be visible to others or physically lost. Deena, an elderly woman, who wrote her passwords on paper, admitted that 'I may have left it on the table, exposed . . . I may have left it there, but I try not to'. Password management is therefore one of the primary examples of how public-access computers produce contexts where literacy and technological knowledge have specific, situated requirements that exceed the literacy requirements for those with a secure digital home.

Some users further relied on staff assistance in place of developing independent digital literacy skills. For example, Jeremy, a staff member, related that

> there was a patron who came in and he was needing to order car parts. He didn't know anything about computers, didn't care . . . I had to sit down with him and basically do it for him, but as soon as we got the car parts he needed up, he was throwing his credit card at me, throwing all the information that that thing needed. He didn't care; he just needed the parts and he wanted to go out the door.

Jeremy also noted that 'there are plenty of patrons that it's really frustrating how many times I have to tell them the exact same stuff', a phenomenon which was also reflected in our participant observations. This could lead to persistent learned reliance on external assistance for computer use in place of the learned digital problem-solving that is increasingly essential for safe and efficacious computer use, as well as employment in many job sectors. This small moment demonstrates that despite access to library computers and support by the library staff, a number of material and behavioral security risks remain, compounding the inequities faced by those with lower technological capital and those experiencing digital home-lessness.

Patrons engage in many risk-mitigating and risk-promoting actions associated with security fatigue resulting from either paranoia or apathy about the daily digital risks they face. This manifests in two ways: those whose resignation to risk promotes continued risky computer behaviors, and those who self-limit and therefore disallow specific computer uses for fear of risk exposure. Jerry is a 30-year-old writer who uses public computers at the library and exhibits behaviors indicative of this resignation to risk on computer platforms. He described this as a kind of 'acceptance':

> The acceptance that as hard as I fight and hard as I try to protect my identity, there's always going to be more clever, with more time and stronger motions, hellbent on getting around whatever I'm doing. If major corporations can get hacked and millions of emails and accounts get leaked, what the hell am I going to do? I can use a VPN service, I could be more careful about what websites I go to, sure. But if, and when, it happens, it will have been an inevitability of just being on the internet in the first place.

In this context, Jerry expresses a common refrain among computer users in our study: a view that individual Internet behaviors are helpless against the myriad bad actors who may be out there to steal PII or otherwise produce harms. Among our population, this fear was limited to digital bad actors, and few reported fears of the risks associated with, say, printing that same PII in a public context. In this case, Jerry is not able to really address his security concerns because they are both vague and because his behaviors would fall short of those 'more clever' bad actors with 'more time and stronger motions'.

Others experience a similar resignation, but instead respond by over-limiting their behavior. Unlike Jerry, who may be over-exposed to digital risks without interventions, these users are unable to carry out computer tasks which may seem simple and commonplace, for fear that their lack of experience or the presence of bad actors may compromise even these safe computer uses. Consider Linda, a 55-year-old woman who relies on the library for vital Internet access. Linda considers herself resigned to mitigating security risks primarily by disengaging from activities that she imagines could produce risk or allowing friends or family to perform those tasks for her. 'I'm not that very careful. Maybe because I have not handled computers and all and . . . [My daughter] knows a lot of things to do with more than I. I don't handle that much'. This attitude exemplifies the problematic relationship and difficulty of engaging with experiences of (in)security and (in)equality in public computer users. These dual experiences compound one another and produce security fatigue, which in turn reproduces vulnerability and inequality.

Further work is required to better explain and track the precise dual needs of security risk and inequality in public computer users without digital homes.

Conclusion: addressing inequality and remediating digital home-lessness

Digital home-lessness is a multifaceted problem which libraries partially address but do not solve simply by providing public-access computing. Addressing the technological capital inequality alongside the unique and compounding problem of digital home-lessness requires both a social-educational response to address literacy concerns and a technological-material response to address access and capacity for those with low technological capital. We suggest that further research is required to parse both concerns. Our research pushes forward scholarship on digital access and the digital divide by revealing that our users face a range of *infrastructural* problems that extend beyond technical computer systems. Our findings reveal that this experience of digital home-lessness results from intersecting affective, physical, and social forces that are compounded by these users' low technological capital. This article expands the literatures' characterization of user's differential experience of inclusion in light of the digital divide and reveals that avenues toward equity need to consider the uniquely compounding problems resulting from digital home-lessness.

Our findings further advance current literature on the digital divide that simplify the discourse into first-order concerns of access and second-level concerns of literacy by showing how these two concerns coalesce in a compounding experience of digital home-lessness. Our results show how experiences of digital home-lessness cannot be separated into discrete literacy concerns and access concerns, but rather show that these users experience a multiplied inequality that compounds with other existing socioeconomic inequalities they face. For example, our finding that users' risky behavior in online settings is compounded both by low digital literacy and by the unique context by which digital access is mediated shows how first- and second-order access and use concerns cannot always be usefully separated. By examining users' lived experiences, our findings elaborate an *emic* perspective on digital home-lessness. This perspective demonstrates that our users require not only digital literacy, but a specific brand of digital literacy adapted to the many quirks, policies, and physical frameworks that make up public computer stations. Literacy and access are coupled concerns, and remediating either involves the other more directly.

While they add to the discourse on user experiences, these findings do not fully characterize the way access is constructed in library settings and further research is required into the socio-material infrastructure that provides and inhibits access. This avenue is particularly important if this social research is to be made more pragmatic from a remediation or policy perspective. Therefore, a robust consideration from a systems infrastructure approach as informed by our findings on user experiences would be a vital next step if more equitable and accessible broadband Internet systems are to be produced.

We also suggest that further research is needed to evaluate the viability of potential applied outcomes. More rigorous attention to possible interventions is required to address

and remediate the inequalities produced by digital home-lessness. Interventions that join socially situated technical solutions could provide pathways for supplying a digital home many of our participants lack. Other potential interventions are also possible, including digital literacy classes or digital inequality training for technical staff. This exploratory ethnographic research suggests that these pathways forward could not only be generative for a better understanding of the contours of digital inequalities but could also provide material improvements in the lived experience and socioeconomic mobility of a portion of the population whose disadvantages in the job market and elsewhere stem in part from their lack of a secure, usable digital home. Additional research targeting specifics of these interventions and the viability of specific design methods is required to test these suggestions.

Taken together, our work shows that individuals who rely on public-access Internet face intersecting and multiplicative inequalities stemming from the absence of a secure, broadband-enabled device at home. The resulting experience of digital home-lessness reproduces digital and socioeconomic inequalities which are difficult to solve, particularly because these affective and material experiences intersect with a number of specific individual socioeconomic experiences. To address this problem, further interdisciplinary study on the infrastructural systems that inform access is necessary. In addition, novel systems designs targeting inequality remediation are required if a triangulated and targeted remediation of digital home-lessness is desired.

While this work has direct relevance to the widening digital divide in the United States, it also has implications for other contexts, including European contexts, where the digital divide remains pervasive, if less extreme than in the United States. Additional work would be required to draw direct analogs to many other international contexts where library systems and public Internet access face varying degrees of availability and government-level scrutiny. In many countries, home connectivity may be more resource-limited at a public infrastructural level, while for those living under more authoritarian regimes the inequalities faced merely by the lack of VPN availability in public computers would be of much greater concern than in the United States, where government scrutiny of private users is not especially severe. However, when looking beyond the level of direct analog, a key lesson from our findings for a variety of international contexts is the realization that digital inequality at the personal hardware level is a distinctly material and therefore embodied circumstance. The inequalities do not just translate from digital to real-world contexts, rather they originate in material relationships, and this means that remediation of digital inequalities should consider these access concerns in addition to literacy and availability concerns when designing policy interventions that seek to level the digital playing-field.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This material is based on work supported by the National Science Foundation under Grant Nos. #1742815 and #1946180.

ORCID iD


Matt Comi https://orcid.org/0000-0003-0278-856X

References

Ajunwa I, Crawford K and Schultz J (2016) Limitless worker surveillance. Available at: https://mronline.org/wp-content/uploads/2017/12/3Ajunwa-Schultz-Crawford-36.pdf

Andrejevic M (2014) The big data divide. *International Journal of Communication* 81: 673–689.

Baek YM (2014) Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behavior* 38: 33–42.

Barocas S and Selbst AD (2016) Big data's disparate impact. *California Law Review* 104(3): 671–732.

Becker S, Crandall MD, Fisher KE, et al. (2010) Opportunity for all: How the American Public Benefits from Internet Access at U.S. Libraries (IMLS-2010-RES-0).

Bernard HR (2011 [1940]) *Research Methods in Anthropology Qualitative and Quantitative Approaches*, 5th edn. Lanham, MD: Lanham, MD: AltaMira.

Bertot JC, McDermott A, Lincoln R et al. (2012) 2011-2012 Public Library Funding and Technology Access Survey: Survey Findings and Results.

Bruckner MA (2018) The promise and perils of algorithmic lenders' use of big data. *Chicago-Kent Law Review* 93: 3–60.

Carlson A and Isaacs AM (2018) Technological capital: An alternative to the digital divide. *Journal of Applied Communication Research* 46(2): 243–265.

Crawford S (2014) Libraries struggle to close the 'digital divide'. *Nytimes.com*. Available at: https://www.nytimes.com/roomfordebate/2012/12/27/do-we-still-need-libraries/libraries-struggle-to-close-the-digital-divide (accessed 15 January 2019).

Dailey D, Bryne A, Powell A et al. (2010) *Broadband Adoption in Low-income Communities*. New York: Social Science Research Council.

Edelman BG and Luca M (2014) *Digital discrimination: The case of 'Airbnb.com'*. Harvard Business School NOM Unit working paper no. 14-054. Cambridge, MA: Harvard Business School.

Fisher LE (2009) Target marketing of subprime loans: Racialized consumer fraud & reverse redlining symposium. *Journal of Law and Policy* 18: 121–155.

Foucault M (1977) *Discipline and Punish: The Birth of the Prison*, 1st American edn. New York: Pantheon Books.

Fuchs C (2013) Societal and ideological impacts of deep packet inspection internet surveillance. *Information, Communication & Society* 16(8): 1328–1359.

Gandy OH (1993) *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview.

Gangadharan SP (2013) *Joining the Surveillance Society? New Internet Users in an Age of Tracking*. Washington, DC: New America Foundation.

Gangadharan SP (2017) The downside of digital inclusion: Expectations and experiences of privacy and surveillance among marginal internet users. *New Media & Society* 19(4): 597–615.

Gumbus A and Grodzinsky F (2015) Era of big data: Danger of discrimination. *ACM SIGCAS Computers & Society* 45(3): 118–125.

Halford S and Savage M (2010) Reconceptualizing digital social inequality. *Information, Communication & Society* 13(7): 937–955.

Hannak A, Soeller G, Lazer D et al. (2014) Measuring price discrimination and steering on e-commerce web sites. In: *Proceedings of the 2014 conference on Internet measurement*, Vancouver, BC, Canada: ACM Press, pp.305–318.

Lofland J, Snow DA, Anderson L et al. (2006) *Analyzing Social Settings: A Guide to Qualitative Observation and Analysis*, 4th edn. Belmont, CA: Wadsworth/Thomson Learning.

Lyon D (ed.) (2003) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London; New York: Routledge.

Madden M (2017) *Privacy, Security, and Digital Inequality How Technology Experiences and Resources Vary by Socioeconomic Status, Race, and Ethnicity*. New York: Data & Society Research Institute.

Madden M, Gilman M, Levy K et al. (2017) Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review* 95(1): 53–126.
Madianou M (2015) Digital inequality and second-order disasters: Social media in the typhoon Haiyan recovery. *Social Media + Society* 1(2): 603386.
Narayanan A (2011) There is no such thing as anonymous online tracking. The Center for Internet and Society, Stanford Law School. Available at: /blog/2011/07/there-no-such-thing-anonymous-online-tracking (accessed 24 October 2014).
Newman N (2014) How big data enables economic harm to consumers, especially to low- income and other vulnerable sectors of the population. *Journal of Internet Law* 18(6): 11–23.
Nissenbaum HF (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.
Ohm P (2010) Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review* 57(6): 1701–1778.
Pasquale F (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.
Pew Research Center (2018) *Demographics of Internet and Home Broadband Usage in the United States*. Washington, DC: Pew Research Center.
Prince D (2018) Cybersecurity: The security and protection challenges of our digital world. *Computer* 51(4): 16–19.
Ragin CC, Nagel J and White P (2004) *Scientific Foundations of Qualitative Research. Report on the National Science Foundation Workshop on Scientific Foundations of Qualitative Research, July 2003*. Arlington, VA: National Science Foundation.
Roth S and Luczak-Roesch M (2020) Deconstructing the data life-cycle in digital humanitarianism. *Information, Communication & Society* 23(4): 555–571.
Selwyn N (2004) Reconsidering political and popular understandings of the digital divide. *New Media & Society* 6(3): 341–362.
Smith A (2017) *Americans and Cybersecurity*. Washington, DC: Pew Research Center.
Staples WG (2014) *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. Lanham, MD: Rowman & Littlefield.
U.S. Council of Economic Advisers (2016) *The Digital Divide and Economic Benefits of Broadband Access*. Washington, DC: U.S. Council of Economic Advisers.
Van Maanen J (2011) *Tales of the Field: On Writing Ethnography*, 2nd edn. Chicago, IL: University of Chicago Press.
Warren CAB and Karner TX (2015) *Discovering Qualitative Methods: Ethnography, Interviews, Documents, and Images*, 3rd edn. New York: Oxford University Press.

Author biographies

Matt Comi completed his PhD in Sociology at the University of Kansas during the review of this manuscript and is now the Frank and Betty Koller Postdoctoral Fellow at the National Farm Medicine Center.

Sarah Smith completed her PhD in Sociology at the University of Kansas during the review of this manuscript and is currently a Social Science Research Analyst at the Department of Health and Human Services

Walter A Goettlich is a PhD Candidate in Sociology at the University of Kansas.

Perry Alexander is the AT&T Foundation Distinguished Professor of Electrical Engineering and Computer Science and Director of the Information and Telecommunication Technology Center at the University of Kansas

Drew Davidson is an Assistant Professor in Computer Science at the Information and Telecommunication Technology Center at the University of Kansas

William G Staples is a Professor Emeritus of Sociology and Director of the Surveillance Studies Research Center at the University of Kansas

Résumé
Aux États-Unis, des millions de personnes qui n'ont pas d'ordinateur ou de connexion à haut débit à leur domicile doivent compter sur les bibliothèques publiques pour accéder à Internet. À partir d'un vaste ensemble de données d'entretiens et d'observation participante dans trois bibliothèques publiques, nous analysons la manière dont ces personnes s'y retrouvent dans ces environnements complexes et comment ceux-ci influent profondément sur leur vie et expérience numériques, que nous qualifions de *sans-abrisme numérique* (*digital homelessness*). Nous identifions ici trois thèmes qui caractérisent le rapport entre l'utilisation de l'ordinateur en bibliothèque et le sans-abrisme numérique: la *bouée de sauvetage* englobe l'ensemble des activités qui nécessitent l'accès à un ordinateur et au haut débit; la *négociation de l'accès* se concentre sur les désavantages en matière d'utilisation, de confidentialité et de sécurité pour ces utilisateurs; et les *activités risquées* concernent la multiplicité des usages d'Internet et informatiques non sécurisés qui se trouvent exacerbés par un faible capital technologique. Nos résultats permettent d'avancer dans l'étude de la fracture numérique en mettant en lumière la manière dont l'expérience du sans-abrisme numérique limite l'inclusion sociale et reproduit les inégalités socio-économiques.

Mots-clés
accès à Internet, capital technologique, fracture numérique, inégalités, surveillance

Resumen
En Estados Unidos, millones de personas que no tienen un ordenador o banda ancha en su vivienda deben hacer uso de las bibliotecas públicas para acceder a internet. A partir de una extensa base de datos de entrevistas y observación participante en tres bibliotecas públicas, en este artículo se analiza cómo las personas se orientan en estos entornos complejos y cómo éstos moldean profundamente sus vidas y experiencias digitales, las cuales se caracterizan como *sinhogarismo digital*. En el artículo, se identifican tres temas que caracterizan la relación entre el uso de ordenadores en la biblioteca y el sinhogarismo digital: el *salvavidas* abarca el conjunto de actividades diversas que requieren acceso a ordenadores y banda ancha, la *negociación del acceso* se centra en las desventajas de uso, privacidad y seguridad entre estos usuarios y las *actividades de riesgo* se concentra en la multiplicidad de prácticas informáticas y de internet que son inseguras y se ven exacerbadas por el bajo capital tecnológico. Nuestros resultados suponen un impulso para la literatura sobre la brecha digital al arrojar luz sobre cómo la experiencia del sinhogarismo digital limita la inclusión social y reproduce la desigualdad socioeconómica.

Palabras clave
acceso a internet, brecha digital, capital tecnológico, desigualdad, vigilancia