The downside of digital inclusion: expectations and experiences of privacy and surveillance among marginal internet users

The Downside of Digital Inclusion: Expectations and Experiences of Privacy and Surveillance among Marginal Internet Users

Although digital inclusion research has come a long way since its initial techno-deterministic assumptions, very few studies in this domain have addressed the extent to which pervasive digital tracking and targeting, by both state and corporate actors, might contribute to conditions of unfairness and inequality in society. In the United States, this gap is particularly pronounced as technology companies assume a greater share of responsibility in bridging the so-called digital divide. Corporate-supported digital inclusion programs do not have a reputation of protecting or informing users who may be targeted by automatable, algorithmically driven processes that predict user behavior (hereafter, "data profiling").[1] These efforts to provide digital literacy and public access to the Internet and digital devices ("broadband adoption") fail to engage issues of users' digital privacy or the appropriateness of how digital information is shared and flows (Nissenbaum, 2010) and neglect topics of surveillance and the collection and monitoring of personal information for the purposes of social control (Gandy, 2009; Lyon, 2001; Marx, 1985).

While all citizens and consumers are affected by shifts in the meaning and nature of privacy and surveillance, members of underserved communities—that is, groups that have been historically marginalized, such as poor people, people of color, immigrants, and indigenous peoples confronting social and economic injustice (Fraser, 2003)—face greater risk than most: in the process of data profiling members of marginalized groups, corporations and the state can exacerbate existing conditions of inequity. From data

collection to data sharing to data analysis, members of historically marginalized groups are at risk of being stereotyped, exploited, or alienated. As members of marginalized groups are tracked, categorized, and targeted, corporations and states can use and reuse these data profiles, creating a "feedback loop of injustice" (Hamid Khan in Bond et al., 2014).

Beginning with the premise that community anchor institutions play a critical role in shaping individual and community expectations of broadband technologies (Dailey et al., 2010), the current study peers into broadband adoption programs at community-based and public institutions ("digital inclusion providers") in order to understand the ways in which privacy and surveillance issues emerge and are engaged in these settings. It focuses on marginal Internet users (or "marginal users"), which refers to members of historically marginalized groups typically targeted by digital literacy programs. How do marginal Internet users negotiate norms, expectations, and practices regarding information flows when learning about broadband technologies? By presenting the findings of a mixed-methods study of digital inclusion programs, this article sheds light on the nature and meaning of digital inclusion in an era of pervasive tracking and targeting. It demonstrates tensions between the promise of broadband opportunities and the threat of inappropriate and asymmetrical flows of information, and in so doing, identifies a policy opportunity to guard against privacy and data profiling problems faced by individuals, including those with low levels of technical savvy.

Overview: Digital Inclusion's Disconnect from Privacy and Profiling Concerns

Many policymakers and advocates for digital inclusion hold an uncomplicated view of broadband as a pathway to opportunity for the underserved (Selwyn, 2004). In

2009, for example, the United States Congress established the Broadband Technology Opportunities Program (BTOP), pouring approximately $450 million into public computing and digital literacy programs across the country to address disparities in access and use and to "spur job creation and stimulate long-term economic growth and opportunity" (U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA), 2009a: 1). Broadband was seen as having "transformative power" to lay the foundation for people's "long-term prosperity" (Seifert, 2009), and Vice President Joseph Biden stated that the programs served as a "down payment on the President's commitment to bringing educational and economic benefits of the Internet to all communities" (Biden in Kang, 2009).

As President Obama's second term neared, the stakes of broadband adoption remained high, even as BTOP's end became apparent. The president stressed the imperative of "connecting every part of America to the digital age" (Obama, 2011). Government services, such as those offered by the Affordable Care Act, became online-only options (Super, 2014), and the job market became more digitally dependent. By 2012, 80 percent of Fortune 500 companies, including Walmart, Comcast, and McDonald's, accepted job applications online only (*Science Magazine*, 2013).

The question of digital privacy

Meanwhile, digital privacy "defenders" have argued for adequate privacy protections in the provision of universal broadband. They worry that the capacity of broadband-enabled technologies to collect and exchange consumers' sensitive personal data poses "risks to consumer privacy" and require remedial measures in order to "increase consumer trust and truly achieve broadband's potential" (Center for Democracy

and Technology, et al., 2010: 1). Many privacy rights advocates routinely criticize technology industry players, such as Google, Microsoft, and Comcast, all of which derive enormous profit from invasive collection, sharing, and analysis of personal data (Chester, 2007).

In the privacy field, researchers and advocates highlight practices that leave users in the dark about how corporations collect, share, and analyze user data with impunity. For example, Narayanan's (2011) research details five ways in which third parties (e.g., sites like ad networks that a user involuntarily visits when connecting to a first party content provider) compromise user privacy. Risks arise when first party content providers sell user identities to third parties for a fee, or when first parties leak user identities to third parties by including user names in "http referrers," the addresses of webpages that third parties link to. To the latter, Mayer and Mitchell (2012) demonstrated user name or ID leakages in 61 percent of the top 250 websites (ranked by the Web traffic analysis company, Alexa).[2] Other privacy scholars, like MacDonald and Cranor (2008) and Acquisti and Grossklags (2008), point to the inadequacy of notice-and-consent and other transparency requirements, which fail to inform users about how companies collect, analyze, or share user data with third parties.

While the type of user examined in the above studies tends to be an "average consumer" and the privacy intrusions described can befall any individual, some privacy research seems to suggest that consumers with low socioeconomic status face greater challenges in confronting privacy and surveillance issues. Turow, Meltzer, and Feldman's study (2005) found that survey respondents with only a high school diploma performed worse than graduate degree holders in answering knowledge questions about

privacy. Meanwhile, a Pew Research Center study (2014) reported that adults with college degrees were more likely than other populations to "check up on their own digital footprints" (p. 21).

Digital automation of unfairness

A handful of researchers have begun to consider consequences of surveillance technologies for historically marginalized communities. Gandy (2009) described a process of digitally enabled cumulative disadvantage: automatable statistical analyses of the behavior of particular populations (e.g., African Americans and Latinos as non-affluent consumers who prefer "low brow culture") inform and justify exclusionary policies and practices (e.g., targeting low-quality news products to African Americans and Latinos which in turn excludes them from representation in and access to a market for high quality news). Fisher (2009), Gangadharan (2012), and Pasquale (2014) studied lenders, data brokers, online platforms, and other actors in the data supply chain and their use of digital tracking and algorithmic analysis to identify and target low-credit ranking consumers for risky subprime loans.

While the above scholars worry about data collection and use based on accurate data, others—including those outside of academia—have focused on error in data-driven systems and their impact on the underserved. For instance, several states operate computerized welfare assistance systems programmed with overly stringent criteria, resulting in denial of services to legitimate, qualifying applicants (Woodhouse, 2015; Eubanks, 2013). Meanwhile, E-verify, an automated system of employment verification run by the federal government, routinely misidentifies people with non-Caucasian sounding names as ineligible to work in the United States (Leadership Conference on

Civil and Human Rights, 2014).

Additionally, as Barocas and Selbst (2016) explain, data profiling of underserved populations can arise unintentionally. This occurs when data inputs correlate with particular attributes of the underserved and when data analysis is biased by these proxy inputs.

Research linking digital inclusion to digital harms

Where are digital inclusion researchers and advocates in debates about the dangers of digital society? The few examples of government and civil society survey research specific to digital inclusion do not have consistent views on the importance of privacy and safety concerns in broadband non-adoption. While the surveys conducted by NTIA (2009b, 2011) and Pew Research Center (2013b) ranked privacy and security concerns low on a list of reasons for non-adoption in comparison to other factors like relevance or cost, an FCC study (Horrigan and U.S. Federal Communications Commission (FCC), 2010) showed that nonusers prioritize such risks as a third reason, after cost and comfort.[3]

On the scholarly front, two studies address privacy and surveillance within the context of digital inclusion programs. Viseu, Clement, and Aspinall's (2004) qualitative study of individuals considered to be "on the wrong side of the digital divide" in Canada revealed that interviewees felt a high degree of concern for user privacy, though an equally pronounced sense of resignation to the inevitability of diminished digital privacy.

Eubanks' (2011) ethnography of participants in a community program designed to bridge the digital divide demonstrated that limited or lack of access to the Internet or computers for poor, working class women was a myth. Whether under electronic

surveillance at work or in the welfare office, women's lives were suffused with digital technology over which they had little control. This manner of digital inclusion, Eubanks argued, affected poor and working women's material status, emotional well-being, and political efficacy. Employers deployed monitoring systems that tracked worker activities and prevented women from organizing for better workplace conditions. Case workers in the welfare office relied on computer-driven systems that housed records of women's personal behavior and automated processes of ineligibility.

Taken together, Eubanks' and Viseu et al.'s works raise several instructive points for this study. First, digital inclusion efforts do not offer critical perspective on optimistic statements made by advocates of programs such as BTOP. Though access to computers and the Internet can provide opportunities to members of marginalized communities, opportunities come with risks, including privacy intrusions and social control due to surveillance. Sometimes risks originate from the technologies themselves; in other cases, they extend existing social practices of disciplining poor people and people of color.

Second, privacy concerns do not show up in studies of non-adoption, because many marginal users adopt broadband by necessity, in spite of privacy or surveillance concerns. Few people have the option of staying offline. As Eubanks' study demonstrates, the marginal Internet user is embedded in information and communication infrastructures regardless of personal choice, means, or capabilities.

Third, community anchor institutions play an integral role in shaping marginal users' expectations of broadband technologies. At public computer centers, public libraries, and other community spaces, marginal users negotiate norms, expectations, and practices regarding broadband technologies, including ones related to privacy intrusions

or surveillance.

These points raise several research questions:

- First, what concerns about sharing of information and about privacy or surveillance are arising within the context of learning how to use the Internet and computers?
- Second, in what ways do marginal Internet users face risks related to information sharing?
- Third, in what ways do these privacy risks deter from perceived and actual benefits of using the Internet?

A Study of Privacy and Surveillance in Digital Literacy Settings

Background: A resource gap

A review of one of the field's most prominent resources (digitalliteracy.gov), conducted during the qualitative study described below, provides important context to the study of privacy and surveillance concerns arising in digital literacy organizations. Whether due to benign neglect or intentional oversight,[4] practitioners contributing to the site largely failed to address topics concerning the nature and appropriateness of information flows or information asymmetries.

Established in 2011, and curated by the NTIA, digitalliteracy.gov features hundreds of educational resources posted by government agencies, nongovernmental organizations, and corporations. In January 2012 and then again in March 2013, the author examined "Topics," "Skills," "Resource Formats," and "Audiences" on digitalliteracy.gov, finding that none of the resources grouped under these content headings included privacy or surveillance-related material.

Inspection of all the resources listed on the site yielded a very small number of privacy-related materials, and none related to surveillance or data profiling. In January 2012, eight resources (out of 452) pertained to privacy. Most focused on privacy settings for social network sites and safeguards for children online. In March 2013, the number of resources that featured privacy information increased to 11 (out of 477 or just over 2 percent). While a number of resources concerned youth safety (a total of 42 in March 2013) and digital security (a total of 20 in March 2013), digital literacy programs ignored corporate and government surveillance or tracking technologies altogether. Overall, the snapshot of digitalliteracy.gov illustrates a dearth of educational matter concerning tracking, targeting, and information flows.

Field study design: A mixed methods approach

The study described here took a mixed methods approach to examining four digital literacy institutions serving marginal Internet users. It combined participant observation of students in the classroom with participatory action research to arrive at an understanding of privacy and surveillance. Participant observation, a technique successfully used in studying community technology initiatives (Kvasny, 2006), was chosen for its unobtrusiveness in discovering privacy and surveillance concerns. Participatory action research was chosen for its emphasis on reciprocity and ethical engagement when studying sensitive issues with communities, particularly historically marginalized ones (Kincheloe and McLaren, 1994). Collaborative work entailed the co-creation of privacy learning tools and involved large and small group discussions and, at the behest of one of the participating organizations, one-on-one structured interviews, all of which provided insights and stories of staff working on the front lines with marginal

Internet users (see also Budka et al., 2006; Eubanks, 2011; Masucci and Gilbert, 2011).

During an eighteen-month period (between 2012 and 2013) in major northeastern cities in the US, the author worked with a citywide computer training center, a senior center, a local social movement organization, and a large public library system.[5] Funding for these institutions' programs came primarily from state sources, though technology companies had contributed additional program support at two of the organizations studied. All four organizations predominantly serve members of low-income communities of color, including both American citizens and immigrants. An institutional review board required the author to obtain partnership agreements from each collaborating organization, written consent from staff members, and oral consent from adult learners interested in participating in the study. Study participants were given the option of attending other classes, if they wished to opt out.

In this time period, a variety of artifacts were collected for analysis:

- A mixture of group and individual-level discussions related to the generation of learning tools, involving more than 100 staff members (each of whom, by conservative estimates, interacts with at least 40 marginal users, or a total of 4,000 users in a given year)
- Seventeen class observations (40 adult students and 5 teachers); and
- Three privacy learning tools, coproduced by staff and the author.

The author used a combination of techniques to capture data. For example, the author recorded and transcribed interview material,[6] did direct transcription of group discussions both small and large, produced summaries of "working group" meetings that were then shared with staff members, and took notes of and documented classroom

activities, including lectures, discussion, teaching and learning techniques, and classroom handouts.

Generally guided by Christians and Carey's (1989) criteria for competent qualitative studies, the author then analyzed the material, looking for common themes that highlighted values and practices pertaining to information flows and their appropriateness. Wherever possible, the author triangulated between perceptions or experiences revealed by marginal Internet users and those recounted by staff who worked with them.

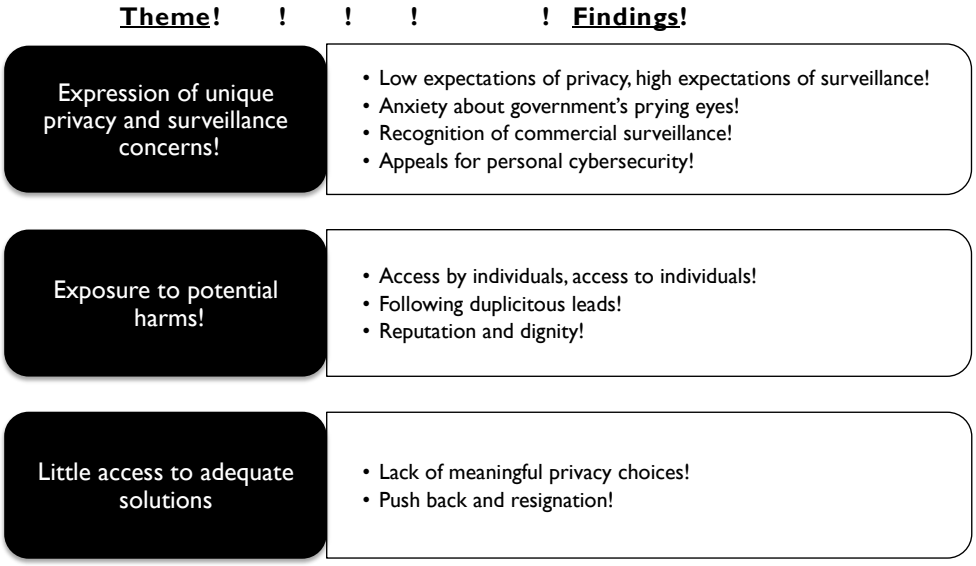
Findings: Marginal users' expectations and experiences

Group discussions, interview materials, and observation of marginal users yielded insights into how the dream of broadband opportunities interacts and sometimes clashes with digital privacy and surveillance concerns. Marginal users believed that broadband adoption would improve basic facets of their lives. With some exceptions (noted below), marginal users felt digital technologies would help them find a job, assist children with their schooling, connect with friends and family, or simply learn something new. To the question, "Does anyone know what the Internet is used for?" the majority of answers of students at the library focused on "finding information" and "look[ing] for a job." At the computer training center, students described the Internet similarly as "a place where you find information" or "find a job," as well as a tool that lets you stay home "to go shopping or do your banking." As one individual at the senior center remarked, "If you don't know the computer, you won't know what's going on in the world or any place else."

But analysis of the activities and dialogue in these digital literacy settings also

reveals that marginal Internet users' privacy and surveillance concerns are central to their early encounters with and expectations of the Internet and computers, though formally absent from digital literacy instruction. Moreover, the digital tools and platforms available to marginal users and the practices they learned exposed them to potential harms of digital tracking and targeting. While informal problem-solving around privacy or surveillance arose in the classroom, solutions available to marginal users did not appear to adequately meet their needs or concerns.

Figure 1. Privacy, surveillance themes among marginal Internet users !



Theme #1: Expression of unique privacy and surveillance concerns

Low expectations of privacy, high expectations of surveillance. Though optimism was apparent, marginal users expressed concerns about privacy and surveillance in ad hoc ways. The threat of digital surveillance and privacy intrusions contributed to their anxieties about broadband.

For most of the marginal users observed in the classroom or recollected by staff, privacy was viewed as a luxury, not a right. At the library, this concern was most pronounced. Staff mentioned how marginal users felt watched, were watched, or seemed as vulnerable as "sheep for slaughter" with respect to protecting personal data. Marginal users' vulnerabilities appeared most acute when applying to and maintaining eligibility in welfare programs, often at the last minute. Not only did users give up intimate details about themselves in exchange for welfare support, they also shared intimate information with staff members, such as email passwords, credit card numbers, or social security numbers. Much in the same way that the poor and working women in Eubanks' study (2012) had to routinely divulge information to caseworkers inputting information into computer terminals, marginal users studied here had little opportunity to limit information flows about themselves.

Anxiety about government's prying eyes. Marginal users worried about government surveillance, mostly stemming from their local experiences with social welfare systems. In some cases, users believed that the digital literacy provider and government entities were complicit in surveillance. For example, at the public library, users could not access unemployment websites, prompting patrons to fault the library for censorship (and not the Department of Labor and its server problems).

Staff regularly received questions about what the library knew about user behavior, such as whether the library truly erased a user's computer usage history at the conclusion of a public terminal session. At the computer training center, instructors reported disinterest in a classroom exercise that involved emailing a local government agency or official. As one instructor said, "A lot of students are hesitant to write to the

mayor or a government official… [P]eople are afraid they're going to get on a list. They don't want to get into any trouble." Because of low participation rates, the center made the exercise optional.

Surprisingly, marginal users did not raise the topic of government surveillance in the context of national security. The lack of salience of privacy versus national security concerns among marginal Internet users suggests government surveillance holds particular meaning for marginal populations. As others have written (Gilliom, 2001, Eubanks, 2011), this meaning ties to a long history of suspicion and monitoring of historically marginalized communities by hegemonic powers.

Recognition of commercial surveillance. Marginal users worried to a lesser degree about commercial surveillance, as compared with welfare state surveillance, though for complex reasons. When students spoke about commercial activities, they expressed concern found in survey research on e-commerce and lower-income populations (Pew Internet & American Life Project, 2010; see also Pew Internet & American Life Project, 2008): users did not trust the safety of websites and felt hesitant to use a credit card online, unless they had a pre-paid credit card.

In general, students rarely learned how to shop online, though occasionally users would exclaim, "I heard you can get good deals on the Internet." When instructors exposed students to e-commerce or discussed it in class, or when staff advised marginal users in one-on-one contexts, students received little guidance about reliable sites (versus predatory or disingenuous ones). Students acquired little information about advertisements, and many struggled to differentiate between advertisements and content online. At the computer center, students learned that search engines listed sponsored links

or advertisements in addition to search results, a process which instructors framed as "more informative."

Marginal Internet users seemed to intuit the reasons for targeting and tracking, despite not knowing about data profiling. At the library, when pop-up ads appeared during a search engine exercise, students experienced advertisers' attempts to grab their attention. In response, one student commented, "Nothing is free in this country." Topics such as recommendation engines did not get addressed, though at the senior center, both students and former students-turned-unpaid volunteers expressed dissatisfaction with niche marketing generally. As one woman said, "We all are targeted, because [companies] do the demographics. They find out who's in the neighborhood, what schools—just a whole lot of information. If you are not in one system, you're in another." Consistent with other studies of poor people (Eubanks, 2011; Gilliom, 2001; Piven and Cloward, 1971), marginal Internet users felt concerned with the ways in which the marketplace and society saw them as second-class citizens. They conveyed a sense of inevitability at the prospect of being "taken for a ride" or targeted.

Pleas for personal cybersecurity. Marginal users' concern for "all the bad things that might happen to you on the Internet" (see FCC, 2010) connected to their desire for a safer Internet experience. They tended to raise questions or share examples of the inappropriateness of information sharing alongside those related to the safety or protection of information online.

In classroom settings at all four organizations, marginal users spoke about identity theft. Most of these stories related to unauthorized use of credit cards and bank accounts, though on occasion, users found themselves the target of phishing attacks. Fraudsters

filled inboxes with messages that lured marginal users with requests for money to, for instance, purportedly help a long lost friend or pay an outstanding parking fine. At the computer center, students spoke at length about Chinese hackers featured in news reports, while at the senior center, older adults worried about predators stalking children. As one user said, "The whole Internet is like the Wild West. There's a lot of bad people out there who are intentionally bad, [and] you just can't see them." The sentiment echoes how some policymakers and advocates have begun connecting the idea of personal cybersecurity to the protection of personal privacy (Gangadharan et al., 2013).

Theme #2: Exposure to potential harms

Access by individuals, access to individuals. Contrary to characterizations by some Internet researchers that public Internet access affords individuals anonymity (e.g., since the computer is not tied to a specific individual; see Pew Research Center, 2013a), users on public computer terminals are not immune to tracking. Computer terminals were configured for Web-based email, and staff taught webmail to marginal users in the classroom. Instructors advised students to always log out of Web-based email or other services at the end of a session, but not after logging into other services and platforms. As Libert (2015) demonstrated, a permanent log-in state facilitates the creation of data profiles, such as in the case of health-related websites that unobtrusively share behavioral data (through referrer urls) with third parties featured on those sites (e.g., a Facebook "Like" button).

Several of the services introduced to marginal users, in particular employment websites like hotjobs.com and Monster.com, required real-name registration. As mentioned above, real-name registration facilitates tracking within a particular site, and

can involve leakage of user data to first and third parties analyzing referrer urls (Mayer, 2012). In this sense, broadband adoption means access by individuals to the Internet, as well as access to individuals by different Internet services and platforms.

Following duplicitous leads. When learning about and accessing broadband, marginal users divulged personal details in commercial contexts that may facilitate harmful targeting or predatory data profiling.

At the library, one user tried a "free" resume service advertised in search results. Under pressure to create a resume for a prospective employer, the user entered personal information including job history and contact information, prompted page by page by the site. On the last page, the service demanded money from the user in order to receive the complete resume. Lacking funds, the user abandoned the effort, left without a resume at the price of his personal information now in possession by the service. Another example revealed at the computer center involved an individual who clicked a link in an email about job searches. The link prompted the student to enter date of birth, address, and phone number, leading to incessant calls asking the student to register for a distance education course. Another individual spoke about Everest, a continuing education company that did frequent targeting: "It's a scam coming up all the time. And that's the price of using the Internet." These cases echo job and education scams cited by regulators and journalists (U.S. Federal Trade Commission, 2012; Wofford, 2013).

Reputation and dignity. Marginal users appeared to have limited control over the construction of digital reputations. The lack of control pertains not only to activities of the marginal individuals as they become active users or adopters, but also to their "pre-adoption" actions or behavior captured and indexed online. For example, at the computer

training center, during a class exercise, an instructor Googled the name of a student, and the person's arrest record from twenty years prior came up as a top result. While neither false nor duplicitous, the search had a destabilizing effect, demonstrating to the user that she did not manage her own digital reputation. The instructor later viewed the experience as an opportunity to teach students "that there's information out there about them."

Though marginal users look forward to expressing themselves and engaging online, Internet services and platforms play an influential role in shaping how individuals become visible online. Search engines, for example, can function as gate-keepers, but both the opacity of companies' proprietary algorithms (Pasquale, 2014) and the complex ways in which user behavior "trains" algorithms to produce particular kinds of outcomes (Hardt, 2014) make it difficult for a marginal user to understand information presented to her—and in this case, about her. Challenging the visibility of an arrest record found through search or preventing others (e.g., future employers) from misinterpreting the significance of a search result is a complicated and sometimes futile process (Crawford and Schulz, 2013; National Consumer Law Center, 2013).

Theme #3: Little access to adequate solutions

Lack of meaningful privacy choices. As mentioned above, marginal users often accessed the Internet with of-the-moment needs. Searching for more secure or privacy-protecting Internet platforms or services was not an option. Users also lacked the digital literacy skills needed to avail themselves of privacy-enhancing technologies. Most students observed in the classroom struggled with basic tasks, such as launching applications or typing a url into a Web browser, versus into a search field of a search engine Web page. Against this backdrop, it is unsurprising that marginal users shared

information, such as in scenarios described above, with little awareness of why information should be collected, how it is used, or whether users should refrain from sharing.

Given research detailing the inscrutability or inefficacy of user agreements for average consumers (Macdonald and Cranor, 2008; Grossklags and Acquisti, 2008), it is also unsurprising that marginal Internet users ignored privacy policies or terms of service agreements that they encountered. When signing up for email, and in spite of instructors' advice to "carefully review" user agreements, students clicked through or past privacy policies and terms of service in order to complete the registration, suggesting these notification mechanisms functioned as meaningless accessories to the new learner's Internet experience.

Push back and resignation. For some marginal users, the threat of insecurity and risk made them abandon the Internet, limit use, or ask others to use the Internet for them. Some marginal Internet users felt unsure of how to best protect themselves and their personal networks (friends and family, especially children) or avoid harmful situations. Expectations of pervasive digital surveillance or low levels of online privacy prompted others to not adopt the Internet, to go online infrequently, or to limit types of online interactions. As one older adult at the senior center recounted, websites "try to extract some information that I don't really want to give up. They want too much info about you. They always want to know your birth date, your age, gender. So, I limit my use of computers." Another individual at the social movement organization balked at Gmail's request for cell phone information during its account registration process. "I don't want an email," he said. "This is too much."

Computers and the Internet raised palpable concerns for many users, even as they learned new skills. Between the prospect of having one's identity stolen—an issue that surfaced in both class observations and group discussions with staff—to receiving unsolicited ads for services and products not needed, to being watched by government, to being hacked, some felt they could never feel safe or protected online and chose to moderate their use, use the Internet by proxy (such as a child or grandchild), or avoid use altogether. For those who expressed anxiety about "all the bad things," most felt resigned and helpless. One student said, "We weren't warned ahead of time what this was going to be like." As another expressed, "You're just going to have to live with it."

Discussion: Making Sense of Privacy-Poor, Surveillance-Rich Broadband Adoption

Digital inclusion and issues of privacy and surveillance interact in complex ways. Despite the framing found in some governmental studies of privacy and broadband adoption, most users' interests in privacy or surveillance did not stand in stark opposition to their interest in broadband. Adopting the Internet did not, for the most part, involve a binary choice. In this study, people "on the wrong side of the digital divide" did not have the luxury of letting privacy or surveillance concerns dictate choices about how to adopt and interact with digital technologies: marginal users had no choice but to depend upon broadband.

While this study was not designed to show systematic effects of "privacy poor, surveillance rich broadband" on marginal users, its findings demonstrate the complexity of digital inclusion: being included means participation in the potentially harmful consequences arising from inappropriate and asymmetric flows of information.

The findings point to three factors shaping marginal users' norms and

expectations:

The importance of context

The discovery of marginal users' concerns should come as no surprise given their sociohistorical context. As Nissenbaum (2010) has outlined, such context plays a critical role in shaping information-sharing norms and expectations that users bring with them as they adopt new technologies. Different from Nissenbaum's focus on privacy, however, the stories and sentiments raised here suggest many norms and expectations pertain to surveillance and corresponding questions of control (or the lack thereof), and not just appropriateness of information flows. Marginal Internet users have endured the prying eye of government officials or authorities, have witnessed others categorize and target them, and expose themselves in order to get by in life. They have been, in some sense, watched by default. Those anxieties and concerns are transposed to the context of learning about broadband technologies and, in turn, influence the kinds of activities that marginal users feel uncomfortable pursuing online—such as emailing a government official or shopping online. Those same anxieties and concerns also constrain individual agency—for example, you might divulge personal details (to a so-called free resume service) in desperation while searching for a job.

Constraints of the learning environment

The ways in which marginal Internet users become familiar with the Internet, its platforms, and services also contributed to norm- and expectation-setting. On the one hand, digital literacy classes primarily focused on skills, not broad understanding. So, marginal users do not learn how information about oneself travels in a networked communications infrastructure, what controls individuals have over that process, or what

impact one's digital profile or digital footprint has on the way others—employers, banks, learning institutions, law enforcement, retailers, and more—interact with you. So, while they might avoid shopping online or emailing government officials, processes of information sharing, aggregation, analysis, and targeting remain invisible or opaque. And while marginal users might bring concerns up in class, staff demonstrated limited capacity to answer questions or provide tips and counsel users.

Technologies' normalizing impact

Technologies themselves play a role in setting marginal users' experience of privacy or surveillance online. As seen in the case of the student whose arrest record surfaced after a simple search engine exercise, marginal users join a Web that makes their lives hypervisible, not an anonymous Web that hides their digital traces or digitized selves. Moreover, marginal users join a Web that requires them to register for accounts with real names, be it a public assistance program, a job search assistant, or email. As several privacy scholars have argued (Solove, 2002; Battelle, 2005; Ohm, 2010), the tethering of people to real name identities or account registration begs the question of whether individuals have adequate control over information flows. Once a company requires log-in credentials, it can rifle through the data trail that one has created, alter data, draw inferences about people, or expose one's data to harmful or risky scenarios.

In this sense, the technologies create the conditions for types of information flows which the marginal user may have little ability to understand, discover, or manipulate. The way that broadband technologies are introduced to new users makes the divulging of personal details appear normal and second nature.

Conclusion: Accounting for Digital Inclusion's Downside

The technosocial factors described above contribute to a complicated portrait of digital harms and digital opportunities. In a binary conception of privacy versus adoption, the user simply rejects broadband technologies. In a more complex scenario described here, the user adopts broadband technologies with both hope and resignation: a hope that learning how to use email and surf the Web, for example, will lead to better jobs, and resignation that she will encounter some of the same predatory targeting she has experienced before.

In addition, this study points to an interaction between low digital literacy and behaviors that heighten the potential for harm. As mentioned above, marginal users could not easily detect bad or illegitimate actors, struggled to perform basic Internet tasks, failed to distinguish between advertisements and content, and failed to understand the difference between being logged in and logged out. These activities left marginal users exposed and vulnerable to various forms of profiling (e.g., committed by corporate, government, or bad actors) that target unwitting users for both intentionally and unintentionally harmful purposes.

The study also shows an interaction between social status of marginalized individuals and a particular type of Internet tailored for and targeted at the marginal user. As suggested in the example of a student discovering her arrest records during a search engine exercise, the Internet (and the society of users that interacts with it) "sees" the marginal user in a specific way, as an individual whose most important digital instantiation is one that pertains to incarceration. And while the Internet "sees" all individuals in particular ways, marginalized populations are less likely to have the means

to meaningfully challenge these profiles (see Pasquale, 2014). In the future, additional research is needed to better understand sorting processes that categorize marginal users and fuel algorithmic determinations of their digital reputations, whether for ads, credit scores or other "worthiness" scores, and content.

The Role of Policy in Addressing Privacy-Poor Broadband

While these critiques might seem to fault the institutions providing digital literacy and public Internet, they are really an indictment of broader and systemic failures in technology policy. First, digital inclusion policies, from conventional efforts at the FCC and NTIA to lesser known initiatives at the Department of Health and Human Services, Department of Education, and Federal Reserve, have failed to address privacy in a meaningful way that prepares and protects vulnerable populations from the harmful aspects of "being digital." Second, privacy policies, which emanate from a patchwork of regulatory agencies focused on context-specific privacy (health, education, finance, consumer protection, etc.), neglect accessibility questions. The notice-and-consent regime, which undergirds much of privacy regulation, assumes equal ability and resources on the part of users and seldom addresses disadvantaged individuals with low digital literacy levels. Third, innovation policies that pertain to the research and development of secure and privacy-enhancing technologies also neglect considerations of the marginal user (see also Gangadharan, 2013; Gangadharan et al., 2013). Altogether, the development of laws, regulations, or new technologies would benefit those in greatest need of protection.

Though all three kinds of policies will contribute to better outcomes for marginal users, digital inclusion policies may offer the most hope. As noted by the Federal Trade

Commission (2014) in a comment to the FCC, the FCC has sufficient authority under Title 1, Section 706 of the Communications Act to ensure that privacy and security are core features of broadband deployment and adoption efforts. In short, an opportunity exists to marry privacy-enhancing interests with universal broadband goals, as the FCC evolves its regulatory oversight over information services (Stoller, 2014).

Towards Meaningful Digital Inclusion

The organizations that help users adopt broadband routinely engage in processes of setting cultural norms, expectations, and social practices related to the use and non-use of digital technologies. These "digital stewards" answer timely and urgent needs and have the power to steer marginal users to consider a range of solutions. The right regulatory policies can ensure frontline personnel adequately address marginal users' privacy and surveillance concerns.

Marginal users should not have to choose between going online and feeling safe, secure, and free from surveillance. Underserved communities want to benefit from broadband access and wish to partake in the same opportunities afforded by digital technology to other populations. Policies to bridge the digital divide can enable their hopes of reaping the positive benefits of digital inclusion. But until regulators make a strategic effort to do so, this study points to the inadequacy of digital literacy programs in addressing privacy and surveillance concerns of marginal users and helping users to understand the nature of information sharing and information flows online.

---

[1] Examples of corporate-supported digital inclusion programs include internetessentials.com, everyoneon.org, getonlineathome.org, http://wikikc.org/Digital_Inclusion.

[2] See http://www.alexa.com/.

[3] The FCC interpreted the primary reasons according to a different logic than the raw rankings enumerated here: it grouped affordability-related explanations (30 percent of non-users, the first reason); grouped comfort and risk reasons together as "digital literacy" (28 percent, the second reason); and, identified "relevance" (14 percent, the third reason).

[4] The reason for the dearth in attention to privacy by practitioners is an important object of study, though beyond the scope of this paper.

[5] The author contacted a number of organizations involved in digital literacy work, including organizations funded by BTOP, to advertise the study and invite organizations to participate. Five organizations agreed to participate in the study, though one of the groups—an organization that provided digital storytelling and digital literacy training to students and members of immigrant populations—became financially unstable and ceased to exist. Only adult populations were recruited for participation.

[6] One group requested that one-on-one interviews form part of the production process for the learning tool.

References

Acquisti A and Grossklags J (2008) What can behavioral economics teach us about privacy? In: Acquisti A (ed) *Digital Privacy: Theory, Technologies, and Practices*. New York: Auerbach Publications, 363-380.

Barocas S and Selbst A (2016) Big Data's Disparate Impact. *California Law Review*, *104*, 1–62 (accessed 11 September 2015) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899

Battelle J (2005) *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*. New York: Portfolio.

Bond Graham D and Winston A (2014) From Fallujah to San Fernando Valley, Police use analytics to target "high crime" areas. *Truth Out*, 5 March (accessed 26 September 2014) http://www.truth-out.org/news/item/22357-predictive-policing-from-fallujah-to-the-san-fernando-valley-military-grade-software-used-to-wage-wars-abroad-is-making-its-impact-on-americas-streets#

Budka, P., Bell, B., and Fiser, A. (2009). MyKnet.org: How northern Ontario's first nation communities made themselves at home on the World Wide Web. *The Journal of Community Informatics* 5(2) (accessed 13 May 2015) http://ci-journal.net/index.php/ciej/article/view/568/450

Center for Democracy and Technology, Consumer Action, Consumer Federation of America, The Cryptorights Foundation, Inc., National Workrights Institute, Privacy Journal, and Pasquale, FA (2010) Joint Comments of Public Interest

Groups. Washington, DC: Center for Democracy and Technology (accessed 1 September 2015) https://www.cdt.org/files/pdfs/20100122_fcc_general.pdf

Chester J (2007) *Digital Destiny: New Media and The Future of Democracy*. New York: New Press.

Christians CG and Carey JW (1989) The logic and aims of qualitative research. In: Stempel III GH and Westley BH (eds) *Research Methods in Mass Communication*. Englewood Cliffs, NJ: Prentice Hall, 342-357.

Dailey D, Bryne A, Powell A, Karaganis J, Chung J and Social Science Research Council (US) (2010) *Broadband Adoption in Low-income Communities*. Brooklyn, NY: Social Science Research Council.

Duhigg C (2012) How your companies learn your secrets. *The New York Times*, 19 February, p. MM30.

Eubanks V (2011) *Digital Dead End: Fighting for Social Justice in the Information Age*. Cambridge, MA: MIT Press.

Eubanks V (2013) Caseworkers vs. computers. In: *Poptech*, 11 December (accessed April 10, 2015) https://virginiaeubanks.wordpress.com/tag/automated-eligibility-welfare-rights-economic-justice/

Eubanks V (2014) Want to predict the future of surveillance? Ask poor communities. *The American Prospect*, 15 January (accessed 26 September 2014) http://prospect.org/article/want-predict-future-surveillance-ask-poor-communities

Fisher L (2009) Target marketing of subprime loans: Racialized consumer fraud & reverse redlining. *Brooklyn Law Journal* 18(1): 121-155.

Fraser N (2013) "Social justice in the age of identity politics: Redistribution, recognition, and participation." In: Fraser N, Honneth A (eds) *Redistribution or Recognition? A Political-Philosophical Exchange*. New York: Verso, 7-109.

Gandy OH (2009) *Coming to Terms with Chance Engaging Rational Discrimination and Cumulative Disadvantage*. Farnham: Ashgate.

Gangadharan SP (2012) Digital inclusion and data profiling. *First Monday*, 17(5) (accessed 29 September 2015) http://firstmonday.org/ojs/index.php/fm/article/view/3821/3199

Gangadharan SP (2013) *Joining the Surveillance Society?* Washington, DC: New America Foundation.

Gangadharan SP, Dosono B and Ngu K (2013) *Virtually Unused: Virtual Private Networks and Public Internet Users*. Washington, DC: New America Foundation.

Gilbert MR and Masucci M (2011) *Information and Communication Technology Geographies: Strategies for Bridging the Digital Divide*. Kelowna, British Columbia: Praxis (e)Press.

Gilliom J (2001) *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. Chicago: University of Chicago Press.

Hardt M (2014) How big data is unfair. *Medium*, 24 September (accessed 24 October

2014) https://medium.com/@mrtz/how-big-data-is-unfair-9aa544d739de

Horrigan JB and U.S. Federal Communications Commission (2010) *Broadband Adoption and Use in America. OBI Working Paper Series No. 1*. Washington, DC: FCC.

Kang C (2009) Biden announces $4 billion in grants and loans in first round of funding for broadband expansion. *Washington Post*, July 2 (accessed 6 April 2015) http://wapo.st/1IDr2le

Kvasny, L (2006). Cultural (Re)production of digital inequality in a US community technology initiative. *Information, Communication & Society*, 9(2), 160-181.

Leadership Conference on Civil and Human Rights (2014). *Civil rights and Big Data: Background Material* (accessed April 14, 2015) http://www.civilrights.org/press/2014/civil-rights-and-big-data.html

Libert T (2015) Privacy implications of health information seeking on the Web. *Communications of the ACM* 58(3): 68-77.

Lyon D (2001) *The Surveillance Society: Monitoring Everyday Life*. Buckingham, United Kingdom: Open University.

Macdonald AM and Cranor LF (2008) The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 4(3): 540-565.

Marx, GT (1985) I'll be watching you. *Dissent* 32(Winter): 26-34.

Mayer JR (2012) Safari trackers. In: *The Center for Internet & Society* (accessed 13 May 2015) https://cyberlaw.stanford.edu/blog/2012/02/safari-trackers

Mayer JR and Mitchell JC (2012) Third-party Web tracking: Policy and technology. *Security and Privacy, 2012 IEEE Symposium*: 413-427.

Narayanan A (2011) There is no such thing as anonymous online tracking. In: *The Center for Internet & Society* (accessed 24 October 2014) https://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking

Nissenbaum HF (2010) *Privacy in Context Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.

Obama BH (2011). *Remarks by the President in State of Union Address* (accessed 24 April 2014) https://www.whitehouse.gov/the-press-office/2011/01/25/remarks-president-state-union-address

Ohm P (2010) Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review* 57: 1701-1777.

Pasquale F (2014) *Black Box Society: The Secrets That Control Money and Information*. Cambridge: Harvard University Press.

Pew Internet & American Life Project (2008) *Online Shopping* (accessed 26 September 2014) http://www.pewinternet.org/2008/02/13/online-shopping/

Pew Internet & American Life Project (2010) *65% of Internet Users Have Paid for Online Content* (accessed 26 September 2014) http://www.pewinternet.org/files/old-media//Files/Reports/2010/PIP-Paying-for-

Online-Content_final.pdf

Pew Research Center (2013a) *Anonymity, Privacy, and Security Online*, 5 September http://pewinternet.org/Reports/2013/Anonymity-online.aspx

Pew Research Center (2013b) *Who's Not Online and Why*, 25 September (accessed 26 September 2014) http://www.pewinternet.org/2013/09/25/whos-not-online-and-why/

Pew Research Center (2014) *Public Perceptions of Privacy and Security in the Post-Snowden Era*, 12 November (accessed 10 April 2015) http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf

Piven FF and Cloward RA (1971) *Regulating the Poor: The Functions of Public Welfare*. New York, Pantheon Books.

Science Magazine (2013) Online job ads report vs. Bureau of Labor Statistics report: Half-full, half-empty. In: *Science Career Blogs*, 6 July (accessed 26 September 2014) http://blogs.sciencemag.org/sciencecareers/2012/07/online-job-ads-1.html

Seifert M (2009) *Testimony. Hearing on Oversight of the American Recovery and Reinvestment Act of 2009: Broadband*, 2 April (accessed 6 April 2015) http://www.ntia.doc.gov/legacy/congress/2009/NTIA_Seifert_Testimony_20090402.html

Selwyn N (2004) Reconsidering political and popular understandings of the digital

divide. *New Media & Society* 6(3): 341-362.

Solove D (2002) Digital dossiers and the dissipation of the Fourth Amendment. *Southern California Law Review* 75: 1083-1168.

Stoller M (2014) The plot to maim Google: How AT&T and Comcast plan to upend the Internet. *Salon*, 17 October (accessed 29 September 2014) http://www.salon.com/2014/10/17/the_plot_to_maim_google_how_att_and_comcast_plan_to_upend_the_internet/

Super D (2014) An error message for the poor. *The New York Times*, 4 January, p. A19.

Turow J, Feldman L, and Meltzer K (2005) *Open to Exploitation: American Shoppers Online and Offline*. Report, Annenberg Public Policy Center of the University of Pennsylvania (accessed 16 March 2015) http://repository.upenn.edu/asc_papers/35

U.S. Department of Commerce, National Telecommunications and Information Administration (2009a) *Broadband Technology Opportunities Program Notice of Funds Availability—Fact Sheet*. Washington, DC: NTIA.

U.S. Department of Commerce, National Telecommunications and Information Administration (2009b) *Exploring a Digital Nation: Home Broadband Internet Adoption in the United States*. Washington, DC: NTIA.

U.S. Department of Commerce, National Telecommunications and Information Administration (2011) *Exploring the Digital Nation. America's Emerging Online*

Experience. Washington, DC: NTIA.

U.S. Federal Communications Commission (2011) *FCC Creates Connect America Fund to Expand Broadband, Create Jobs* (accessed 6 April 2015) https://www.fcc.gov/document/fcc-creates-connect-america-fund-expand-broadband-create-jobs

U.S. Federal Trade Commission (2012) *Diploma Mills*, July (accessed 30 October 2014) http://www.consumer.ftc.gov/articles/0206-diploma-mills

U.S. Federal Trade Commission (2014) *In the Matter of Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*. Washington, DC: FTC.

Viseu A, Cement A and Aspinall J (2004) Situating Privacy Online. *Information, Communication & Society* 7(1): 92-114.

Wofford C (2013) This Veterans Day, Help a vet avoid a GI Bill scam. *U.S. News & World Report*, 11 November (30 October 2014) http://www.usnews.com/opinion/blogs/carrie-wofford/2013/11/11/this-veterans-day-help-a-vet-avoid-a-gi-bill-for-profit-college-scam

Woodhouse M (2015). Antifraud effort on food stamps hurts the poor, advocates say. *Boston Globe*, 27 March, p. A1.

Figure 1. Privacy, surveillance themes among marginal Internet users !