NEW AMERICA FOUNDATION

JOINING THE SURVEILLANCE SOCIETY?

New Internet Users in an Age of Tracking

BY SEETA PEÑA GANGADHARAN*, OPEN TECHNOLOGY INSTITUTE

SEPTEMBER 2013

Recent digital inclusion policies that aim to increase digital literacy of new Internet and computer users, promote civic engagement, and improve economic development do not currently address the privacy needs of new users. This paper presents an in-depth look at surveillance and privacy problems faced by individuals who turn to digital literacy organizations for training and Internet access, including low income individuals, people of color, immigrants, the elderly, and non-English speakers. These individuals are coming online without adequate skills, know-how, and social support to confront digitally enabled government surveillance and corporate intrusions of personal privacy. The paper also details the challenges, such as limited resources, time, and expertise, that providers face when teaching users how to stay safe online. New Internet users should not have to choose between going online and feeling safe, secure, and free from surveillance. Now, more than ever, digital inclusion policies need to pay greater attention to developing providers' expertise and capacity to handle privacy and surveillance concerns of new Internet users. Privacy advocates and developers also have a role to play. Expanding "digital literacy" to include privacy education requires that privacy protecting tools become easier to use. Until then, the benefits of digital inclusion are at odds with the potential harms wrought by a surveillance society.

In the past year, reports of dragnet surveillance by law enforcement and intelligence agencies, widespread consumer targeting, and misuse of big data have alerted the public to the links between online privacy, surveillance, and discrimination. Whether initiated by government or corporate entities, data collection, processing, and profiling now touches all individuals who belong to our computerized, digital society.

As tracking and targeting practices become more widespread, members of underserved communities—typically the poor, communities of color, immigrants, and indigenous groups—may be at greater risk of data-driven discrimination than other Internet users. Individuals from these communities have historically suffered from analog forms of data profiling, such as racial profiling, real estate and insurance redlining,

---

* Seeta Peña Gangadharan is a Senior Research Fellow with the Open Technology Institute. The author thanks colleagues at OTI and Yale Information Society Project for feedback and insights.

predatory lending, political intimidation, and more.

At the same time that systems of data-driven discrimination are expanding, decision makers have identified digital inclusion initiatives as a means to help these very same vulnerable groups learn how to use the Internet and computers, and take advantage of online economic, social, and political opportunities. Whether motivated by public policies or profit, these efforts promise to help increase employment and education levels, inspire civic participation, and contribute to the 21st century information economy.

But if online privacy and surveillance problems are increasing, and the discriminatory effects of data profiling are becoming evermore apparent, what does being digitally included mean? When and how do the threats of surveillance and privacy invasions interact with these individuals' ability to benefit from access to the Internet?

In this report, the Open Technology Institute answers these questions based on original research completed in collaboration with digital literacy training organizations. The study results demonstrate that marginal Internet users—defined here as individuals targeted by digital inclusion efforts—are not prepared to confront the challenges posed by digital surveillance. While users are motivated to learn about the Internet and express concern about many different forms of online surveillance, they and the digital literacy institutions that serve them lack the time and resources to tackle privacy problems associated with participating in new online worlds.

Background

Privacy research has shown that ordinary consumers exist in surveillance-rich environments. A study completed at the University of California showed that Alexa's top 100 websites contain nearly 5,000 third-party tracking files.[1] An older report published by the *Wall Street Journal* identified more than 3,000 tracking files (though not delineated between first- and third-party trackers) for ComScore's top 50 websites.[2]

Studies also show that average Internet users care about privacy, and sometimes try to protect themselves.[3] But technical and behavioral research has revealed that some tools fail to protect users,[4] and users overestimate the degree to which they control their privacy.[5]

Until now, most policy studies of digital inclusion have neglected the particularities of privacy and surveillance challenges faced by marginal Internet users.

In its routine survey about broadband adoption, Pew Research Center's Internet and American Life program just added privacy concerns to a set of reasons that explain why respondents do not use the Internet.[6] The NTIA's 2011 extensive national supplemental survey on broadband adoption only began including privacy and security concerns as one of several reasons for not adopting broadband.[7] The FCC's 2010 consumer broadband study referred to privacy-related issues in response options for two questions (also a lengthy survey) focused on broadband adoption.[8]

The three surveys present potentially conflicting results. Pew reported that 3 percent of respondents chose "Worried about privacy/viruses/spam /spyware/hackers" as a reason for not using the Internet. Most respondents chose "Just not interested," "Don't have a computer," or "Too difficult or frustrating," as an answer. For the NTIA survey, only 1 percent of respondents chose "Privacy and security concerns" as a reason for not adopting broadband in the home. The majority of respondents selected reasons including "Don't need it, not interested," "Too expensive," or "No computer or computer inadequate." By contrast, findings from the FCC survey suggested a potential interaction between online privacy concerns and digital inclusion: the survey showed that 47 percent of respondents were afraid of "all the bad things that can happen on the Internet."[9]

In contrast to digital divide studies, the field of privacy includes a small body of research focused on online privacy, surveillance, and historically marginalized communities. This empirical work speaks to the negative consequences that result from various forms of tracking and monitoring by corporate and government actors and that disproportionately affect the underserved. For example, corporations differentially price and target products to customers who match particular data profiles, a practice that can lead to predatory behavior.[10] One of the most egregious examples of data profiling took place in the 2000s, when subprime lenders targeted African Americans and Latinos, monitoring their online behavior and plying them with toxic financial products.[11]

Another body of evidence questions the neutrality of search algorithms and identifies ways in which statistical aggregations magnify racial stereotypes. A study conducted at Harvard University showed how search engine queries for "African American sounding" names yield advertisements for criminal background checks. Searches for "Caucasian sounding" names do not.[12] Members of communities of color and immigrants, more broadly, face data-driven discrimination in the workplace. As prospective employers turn to credit ratings, e-scores, and databases that catalog individuals' legal residence status, a growing trade in personal data may disadvantage or disfavor Blacks, Latinos, or those with "ethnic sounding" names who are searching for employment.[13]

In the realm of government surveillance, much of the evidence stems from journalistic forays into the extent of massive surveillance programs, including how digitally enabled tracking, storage, and sharing creates the conditions for abusive and overbroad actions by law enforcement and intelligence forces. Police operating under the auspices of anti-terrorism have monitored entire ethnic communities without probable cause, collecting vast amounts of data without warrants and collating the information with publicly and privately available data.[14] Meanwhile, police working to disrupt drug trade have used (with questionable constitutionality) data collected by other agencies, such as the National Security Administration, continuing a decades long tradition of targeting low-income communities of color.[15]

Outside of law enforcement, a government-run (or government contracted) system of public benefits has also taken its toll on the underserved. A digital system of monitoring of participants in social welfare programs deprives the underserved of control over private, day-to-day routines, leading them to associate technology access with the loss of personal dignity.[16]

The Study

Taking its cues from many of the studies mentioned above, the current study sets out to provide a granular understanding of the privacy norms, expectations, and experiences of marginal Internet users. Its descriptive analysis has two primary goals: (1) to bring privacy and surveillance concerns front and center into discussion about digital inclusion, and (2) to bring the difficulties faced by such users to the fore of privacy and surveillance debates.[17] We take a qualitative—or descriptive—approach partly due to the fact that digital inequalities—of access, availability, or skill—are coterminous with other forms of social and economic inequalities. This complex situation makes it difficult to isolate discrete variables that differentiate between cause and effect. These complexities also make it difficult to simulate the marginal Internet user's experience in a laboratory setting for a controlled experiment.

Working In and With Communities

The study examined four organizations which serve different audiences:[18]

- *A citywide computer training center that teaches Internet and computer skills to members of immigrant communities and communities of color.*[19]
- *A senior center, which offers a handful of services, including digital inclusion, to predominantly low-income African Americans, ages fifty-five and up.*
- *A local social movement organization that primarily teaches community journalism to both organizers of and individuals from low-income immigrant communities and communities of color in order to promote economic justice.*
- *A large public library system which provides services, including digital literacy classes, to low-income immigrant communities and communities of color.*

Each organization is based in a major metropolitan city whose population is historically non-white or becoming majority non-white. Two of the four cities have faced severe economic hardship for years, the burden of which falls on low-income communities of color. In total, the groups work with poor people, immigrants, senior citizens, and communities of color, especially Latinos and African Americans. Only adult populations participated in the study.

We invited each group to participate in the study in at least one of three ways designed to elicit (1) the technical context in which tracking of marginal Internet users can take place, and (2) the social context in which marginal Internet users confront or express concerns about online privacy and surveillance and anchor institutions respond to these concerns. These three activities included:

- *providing a list of commonly trafficked websites,*[20]
- *allowing the researcher to observe an introductory digital literacy class for adult students,*
- *working with the researcher to collaboratively create a privacy literacy learning tool.*

Using a list of commonly visited websites, this study established a basic overview of users' Web behavior: what marginal Internet users like to consume online. We also took a snapshot of the degree of commercial tracking embedded in these popular websites, such as third-party tracking software (cookies, flash cookies, html5 local storage software), all of which are known to facilitate the creation of data profiles.

Observation of adult marginal Internet users in the classroom provided a window into the extent to which digital learning does and can entail privacy education. It also helped to identify which privacy and surveillance issues organically arise when individuals are learning to go online for the first time.

As for the participatory portion of the study, the process of collaborating with staff further fleshed out how marginal Internet users encounter privacy and surveillance issues, as well as how they might learn to manage privacy expectations. The process, which included facilitated group discussions and working groups, also provided a window into the ability of digital literacy institutions to address new users' concerns and questions. Like other studies designed in this vein,[21] the participatory method created a more equitable relationship between the researcher and "the researched": staff members worked towards an end product (e.g., privacy literacy tool) intended to be shared with their constituents, in the classroom or otherwise.

By taking a multifaceted approach, this study highlights a range of online privacy and surveillance concerns or problems that arise for new users. It also considers the relative strength of solutions to these problems. In doing so, this report provides vital context too often neglected by other studies.

Field Notes

In total, the author was in the field between January 2012 and June 2013, and completed this analysis on the basis of the following activities:

- *observing 17 classes (roughly 40 students and 5 teachers),*
- *codesigning 3 privacy literacy tools, a process which included a total of 25 group discussions (approximately 100 staff members), 8 one-on-one individual interviews (with seniors, volunteers, and staff), 1 group discussion with 12 digital literacy students,*[22] *and*
- *examining nearly 200 urls commonly visited by public Internet users.*[23]

Challenges

Like all research, this study has its limits. The study's primary challenge is that it does not track harmful effects related to privacy and surveillance issues, such as denial of a loan, experience of predatory lending, price discrimination, loss of one's job, hiring discrimination, chilling of free expression, or political intimidation. The author decided against pinpointing harm, not only because of the issue of time (e.g., many harms arise from cumulative exposure to tracking, targeting, and profiling[24]), but also because of the ethical challenges posed by such research (e.g., at what point should the researcher intervene when study subjects experience harm). Nevertheless, because the study uses multiple methods, it aims to triangulate between data sources and create a full portrait of the privacy landscape for marginal users.

Findings

The activities and opinions of marginal Internet users suggest they have an interest in privacy and surveillance issues, but they may not be aware of challenges specific to the Internet and lack a clear path of action or remedy to potential problems. The study yielded three major findings that reflect upon not only the members of chronically underserved communities, but also the institutions that provide them public Internet access and teach them relevant digital literacy skills.

Finding 1: Marginal Internet users face real, tangible online privacy and surveillance problems.

In this study, we found a different set of conditions facing marginal Internet users. First, though users shared similar Web preferences as compared with average consumers, they evidenced distinctive Web habits. An analysis of popular websites revealed that marginal Internet users gravitated to non-commercial websites that assist with education (e.g., typing tutorials, online dictionaries), computer training (e.g., Microsoft Office certification), and job searches (e.g., Payscroll), not just commercial sites, like Google, Facebook, or Yahoo. They also visited popular sports and entertainment sites, like TMZ, Gossip Center, and Fox Sports, and online lottery and sweepstakes sites.

A scan of third-party cookies using a freely available analytical tool called Netograph,[25] revealed that social gaming sites contained the highest number of third-party tracking files, while a typing tutorial website and Craigslist had none.

Giving Up Privacy Just to Get By

Privacy is a scarce commodity for marginal Internet users. According to staff, because the individuals they serve participated in a social welfare system, they did not have the luxury of privacy and regularly exposed their personal data. People who use digital literacy institutions to gain access to the Internet do so because they often have an urgent task that requires immediate completion. Most commonly, individuals need to fill out forms to remain eligible for different social services—services which are increasingly only offered online.[26] Though these forms require that individuals know how to use a computer and the Internet, many still need staff to help them with navigating a website for a social service agency, purchasing a prepaid mobile phone such as Assurance or Safelink, or filling out a resume and submitting a job application online.

Within these contexts, individuals regularly share personal information with staff members. For example, individuals who have little experience with computers and the Internet request that library staff create, remember, or type in e-mail passwords on their behalf. The same applies for the establishment of online accounts with various services—both commercial and government-run. Individuals also share credit card numbers, social security numbers, phone numbers, addresses, dates of birth, and other personal information as staff members walk them through various websites.

The constrained environment in which marginal Internet users access digital technology corresponds to a situation of diminished power to self-govern and control personal destinies, as described by researchers.[27] While reliance on staff for help also reveals the importance of trusted institutions in helping the underserved go online,[28] marginal Internet users enter into digital society under already unequal conditions of social status.

Other Risks

Marginal Internet users are susceptible to online scams and cannot easily differentiate between first-party content and online advertisements, including ones of questionable legitimacy. Staff members routinely observed individuals entering personal information into websites, which do not always seem legitimate, or observed the byproduct of such activity, such as inboxes flooded with unsolicited e-mails. Class observation demonstrated a variation on the same problem: user confusion about what to click and what not click—in either an e-mail, website, or pop-up. Though instructors would admonish users to only select materials on a Web page they had deliberately visited, users routinely clicked third party content, especially pop-ups or sponsored ad links (i.e., on search result pages).

One staff member shared the story of a user who needed to create a resume quickly. Not having ever completed this task online before, the individual searched for resumes and then clicked a link for a resume-building service, which asked the individual for job history and personal details in a guided, online, page-by-page process. The very last page revealed that the service was pay-to-play, which meant the user, who could not afford to pay, lost his personal information to the service. Another example, revealed in the classroom, involved an individual who clicked a link in an e-mail about job searches. The link prompted him to enter date of birth, address, and phone number, which he thought would help him with a job search. The process instead led to incessant calls asking the student to register for a distance education course.

FINDING 2: MARGINAL INTERNET USERS WANT TO KNOW WHO WATCHES THEM ONLINE, WORRY ABOUT FUTURE HARM DUE TO SURVEILLANCE, AND WISH TO AVOID HARMS.

Like most people, marginal Internet users value their privacy.[29] Whether in class or while accessing the public Internet, users in digital literacy settings questioned who watches them while they conduct their business online. They wondered about surveillance by host institutions, governments, corporations, criminals, or bad actors.

Institutions

At the library, staff reported that individuals who accessed public computers and the Internet wanted to know whether the library logs their activities. When told by staff that the library programs computers to wipe its cache after each user session, many users continued to express doubt. In fact, many libraries—like most institutions—do monitor general traffic patterns in order to maximize network performance. A small but notable number of stories corroborated this monitoring capability, such as when one staff member told the story of the IT department blocking a particular individual from Internet access due to downloading activity.

Government Surveillance

Compared to library Internet users, users at the other organizations were not similarly concerned about monitoring by their host organizations, most likely because they frequent those places to attend classes more so than conduct their own business on public computers on their own time. But broader concerns about government surveillance did arise at all research sites. For example, at the computer training center, staff members reported low participation in an online exercise designed to increase online civic participation of its students. As part of its introductory curriculum, the center required its students to send an e-mail to any city agency or official using the agency's or official's website. Staff members said that a majority of their students refrained from this exercise, due to anxiety over being contacted or targeted by government. Class observation seemed to support this statement, since only about a third of the class at the computer training center completed the assigned task. Some pulled up a city government webpage, leaving it within a minute or two, while others occupied themselves with preceding or pending assignments.

Cybersecurity

Safety and personal cybersecurity come up alongside conversations about privacy.[30] Though public dialogue on privacy typically involves debates about national security, marginal Internet users were more concerned with their own cybersecurity than discussing the country's safety. Only in staff discussions did conversation arise about the tension between fighting terrorism and respecting the privacy rights of citizens.

Instead, a different kind of fear than one related to terrorism captivated users as they learned to go online: fear of technology. While some of this technophobia pertained to a general anxiety about one's ability to learn and conquer technology (e.g., "Will I break the computer if I do X?"), fear also meant trepidation of being exploited, duped, or misled while using a computer and being digitally connected to others. Students in particular worried about identity theft, in part because of prior experiences, such as having a credit card stolen and seeing money disappear from bank accounts.

Students paid close attention to portions of the classes that explained spam, phishing attacks, and viruses. For example, at the computer training center, students talked at great lengths about news stories on television that described bad actors sitting in cybercafés halfway across the world trying to break into people's accounts, e-mail, bank, or otherwise. At the senior center, older marginal Internet users explained that they refrained from online banking or online purchasing, because of past experiences with and fears of future identity theft. Teachers in general repeatedly advised students to log out of user accounts, whether or not computer terminals had a cache-clearing function.

Bad actors also came up in the context of discussing Facebook. Students worried about predators online, especially those that targeted children.

"If you really want it [Facebook], then you better exercise all the privacy they give you and then stick with people you know.

The whole Internet is like the Wild West. There's a lot of bad people out there who are intentionally bad, you just can't see them. There's nothing in their e-mail addresses that has like a patch over one eye or a bandit mask or something that says 'Beware' or 'skull and cross bone—this is not a good person,' you know. So you have to just be careful."

Corporate Tracking

Users also raised concerns about corporate tracking—though in subtle and complex ways. In the classroom, most students expressed an interest in learning and accessing information that helps with employment or educational attainment, while very few people talked about wanting to learn how to shop. However, student discussion revealed that new users are interested in finding good deals through the Internet and getting and using coupons.

When learning about the ad-supported nature of the Internet, students expressed wariness over the truthfulness of ads. But they were not surprised at the role of advertising.

"Nothing is free in this country."

They also seem unsurprised at the fact that different companies try to figure out what users like or might buy and target them accordingly. At the library, students made sense of corporate advertising and tracking by talking about the similarities between pop-up ads, TV commercials, and telemarketing calls.

At the same time, however, users got excited about taking advantage of the Internet and Internet-based tools in order to see themselves. At the social movement organization, students criticized Google when conducting an exercise using Google Maps—not for taking and displaying photos of their places of residence, but for not having up-to-date enough images. They were excited about Google's product.

"That's not what [my house] looks like."

Such behavior reveals a complex set of attitudes towards corporate tracking, rather than a simple binary of "yes" or "no" in relation to data collection, profiling, or targeting done by companies.

Going and Staying Online

In the face of privacy and surveillance concerns, most marginal Internet users want to go online, though they might refrain from certain activities that seem risky. As part of the process of creating a privacy literacy tool, the senior center invited members of its entire community to share sentiments about privacy in one-on-one interviews. This group thus represented the only organization in the study where participants included both public Internet adopters and nonadopters. Two of nine study interviewees at the senior center did not use the Internet, and they revealed that privacy concerns formed part of their reasons for being intimidated by the Internet and not going online. Both individuals spoke about companies and criminals when discussing potential privacy problems of being online. One of them—a South Asian immigrant—cited news stories that investigated cybercriminals and that kept her uninterested in the Internet.

"Daily it comes on TV that with e-mail, people take advantage. And that's not good."

In a similar vein, one instructor talked about students who balked at advice to buy additional software or services that could protect their safety and security. His students said they would rather stay offline than purchase any new items.

But more stories surfaced about refusal of particular types of Internet activities, than outright rejection of the Internet.[31] Whether told firsthand by students or recounted by staff, marginal Internet users talked about not wanting to do online banking or use a credit card for fear of identity theft. This finding is consistent with another survey that talks about lower rates of use among marginal users of online financial management tools and services.[32]

Most who expressed concern or questions about privacy and surveillance did not have an obvious path to resolving those concerns. But they remained hopeful that the Internet could provide them new opportunities to shape their lives for the better. They set aside their concerns in favor of the perceived benefits of quick, abundant information online.

One woman at the senior center quibbled with the idea that surveillance was new for her or her community. She advocated visibility rather than retreat from the Internet.

"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.

I feel that part of my protection is being visible. Being visible on the Internet helps my protection. Because if I am visible, maybe if something happens, somebody will say, 'No, that's not her.'"

Whether defiant, like the above study participant, or resigned and unable to act on privacy concerns, like most others, marginal Internet users felt they needed to stay online, do, and learn more.

FINDING 3: DIGITAL LITERACY INSTITUTIONS STRUGGLE TO MEET THE ONLINE PRIVACY NEEDS OF MARGINAL INTERNET USERS.

Much contemporary discussion about online privacy focuses on end users. Industry associations have invested in extensive public campaigns to teach users about how online advertising works, including how companies track consumers behavior across the Web and use these data to effectively target consumers.[33] A recent survey by Pew Internet & American Life Project showed that average Internet users have taken steps to limit the visibility of their digital footprints. Both age and level of educational attainment affect usage of privacy protecting tools: younger, more educated respondents were more likely to use Virtual Private Networks, anonymizing tools, or encryption software.[34]

Classroom Challenges

In this study, the constraints that students and instructors face at digital literacy organizations make the prospect of teaching and learning about privacy a formidable challenge. Time is tight—both due to the amount of material that teachers try to cover in an introductory class and the pace of digital learning. Within the span of an introductory course, the Internet—what it is and how to use it—constituted one portion of the entire class.

For example, during a five-week course at the social movement organization, Internet instruction took place in two out of five classes. The library had three of its five classes cover the Internet. The computer training center focused half of its 12-week course on Internet-related issues. In each of these settings, teachers attempted to explain key items to students, such as the Internet as a "network of networks," Web browsers, URLs, search engines, e-mail, passwords, and user accounts. Many students were still in the process of figuring out how to use a mouse, move a cursor across a screen, or locate a file folder or a computer program, as they encountered new material and were invited to do things such as open a browser, enter words into the address bar or search engine window, or sending an attachment in an e-mail. Staff expressed that squeezing in another item to teach would be difficult, especially at the library, where the drop-in nature of the course forced the teacher to frequently repeat material from prior sessions.

Learning challenges, such as basic literacy or typing skills, also affected the pace of the classroom. For example, at the library, when asked to type in a food item into a search engine, most students could not spell the word "pineapple." Non-native English speakers met with even more obstacles, such as when Spanish-speaking students conferred with one another to figure out what the instructor had asked before attempting to spell an English word. Password generation—and recall—was also a prominent challenge. At the social movement organization and computer training center, teachers instructed students to combine favorite words and numbers to create a unique password, but the students complained that "unique" and "easily remembered" were at odds with one another.[35] These learning challenges either meant the instructor had to cut material from curriculum or leave students behind in order to cover additional learning objectives.

None of this suggests that marginal users cannot learn about more complicated material: with few exceptions, students displayed high levels of motivation to learn how to navigate the Web, download attachments, use a search engine, and more. But overall, becoming digitally literate takes a significant amount of time that the classroom setting does not easily afford.

Institutional Challenges

On top of the challenges felt at the individual level, institutional capacity shapes the scope and quality of education—privacy or otherwise—available to marginal Internet users. It is worth noting that none of the organizations reported offering privacy education to beginning learners. (The library did offer one-off sessions for privacy and safety on social media, though the class was geared towards teens.) With that said, issues related to information sharing arose in an ad hoc manner in every class observed. As mentioned above, marginal Internet users ask questions about who watches them.

Part of the problem stems from a lack of staff time and resources to develop a deep understanding of online privacy and surveillance, including how governments, corporations, or—in the case of libraries—digital literacy institutions monitor Internet users. Time, in general, is a scarce commodity at digital literacy organizations. Already, most organizations operate on small budgets that are under threat or in the process of being trimmed. The lack of time means staff members cannot apprise themselves of the latest information regarding privacy and surveillance issues. Without dedicated resources, privacy and surveillance problems, concerns, and questions get dealt with in an ad hoc manner, sometimes inaccurately.

In addition, teachers of digital literacy found it difficult to give students definitive answers about the quality of websites. Staff members reported not feeling qualified to say when their opinion of a particular site is good or reliable.

Student: "If I'm looking for something about a medical condition... say I've got high blood pressure, how do I know to link up to one that will give me good info?"

Teacher: "That's a great question. As long as you'll be on the Web, you'll be asking yourself that question."

Student: "Ok. You're telling me there are thousands of sites out there."

When it came to privacy and surveillance related issues, staff members experienced an additional crisis of confidence: they frequently doubted the accuracy of their knowledge about surveillance or privacy invasions.

"I don't think any of us can explain what algorithms do. The concept of tracking is way difficult for us, let alone patrons."

Some staff members revealed that they did not know what cookies are and asked questions as to why a particular company's ads—for example, Staples.com—appeared on one's computer both at work and at home.

As for the organizations that formed staff working groups to collaborate on a privacy learning tool, the process revealed a lack of institutional capacity as well. The social movement organization, for example, engaged in a few discussions to formulate goals for a learning tool, but never completed the end product. Though the senior center and computer training center completed learning tools, they lacked the time and resources to review the material, present to other staff, or implement the tool. Unlike other groups, the library system managed to distribute its learning tool. Without a vetting process for the material, such as by other staff or those more familiar with privacy material, the learning tools appeared to be an unfinished project.

Nevertheless, just as learning challenges did not deter students from wanting to learn, staff members recognized the importance of teaching privacy literacy to students, by teaching themselves about privacy and surveillance problems and solutions in a digital era. Several group discussions revealed a desire to help not only the adult marginal Internet users, but also children. Staff members also wanted to gauge the reliability of privacy enhancing tools and wondered whether the implementation of such tools made them more vulnerable to tracking and targeting. Library staff members wondered whether the library system could stage basic privacy tutorials for employees, including workplace privacy. At the social movement organization, staff members were specifically interested in broadening staff interest in the topic of privacy and surveillance, and finding a specific angle with which to craft future work in this area. Staff at the computer training center and senior center credited the collaborative process for designing a privacy literacy tool with exposing them to new information and wished for more opportunities to learn.

Conclusions: An Inclusive Approach to Privacy

Our goal in this study has been to illuminate privacy and surveillance issues in the context of digital literacy institutions and, conversely, digital inclusion issues for privacy and surveillance debates.

When this study first began, we assumed that we would be working with a range of organizations, which contained both individuals just coming online for the first time, as well as individuals not yet online. Because two organizations dropped out, the study yielded results that pertained more to public Internet adopters, rather than adopters and nonadopters.

Based on the results, this study makes clear that being digitally included is not a straight and narrow path to opportunity and prosperity. Marginal Internet users carry existing inequalities with them into digital environments, including a past history of being surveilled, and they encounter the perils and pitfalls of sharing information when trying to reap the Internet's rewards.

The report had three main findings:
(1) Marginal Internet users face real, tangible online privacy and surveillance problems.
(2) Marginal Internet users care about privacy and want to know who watches them online, worry about future harm due to surveillance, and wish to avoid harms.
(3) Digital literacy institutions struggle to meet the online privacy needs of marginal Internet users.

Because of the challenges of doing research about privacy and surveillance (e.g. the need to monitor and track study participants in order to understand how they experience surveillance), and the innovative nature of this work on marginal Internet users, a call for further research is imperative. The more we know about privacy, surveillance, and historically marginalized communities, the more policymakers can make informed judgments about context-sensitive remedies to a complex online world. Another area of research ought to identify the specific consequences, both immediate and long-term, of data collection, storage, sharing, and analysis on political, economic, and social life of the underserved.

Beyond general research needs, the results presented here have enough consistency to suggest a number of conclusions and recommendations. They are as follows.

First, **marginal Internet users should not have to choose between going online and feeling safe, secure, and free from surveillance.** Policies to bridge the digital divide should uphold their hopes of reaping the positive benefits of digital inclusion. Underserved communities want to go online and wish to partake in the same opportunities afforded by digital technology to other populations. This study points to the need for ethical digital inclusion—where members of underserved communities are hospitably welcome into online environments, rather than exploited in them.

Second, **digital inclusion initiatives need to pay more attention to developing expertise among providers to handle privacy and surveillance questions and concerns that arise in the process of becoming digitally literate.** This study found that there is no shortage of interest in privacy education—either among marginal Internet users or staff. Though we worked with digital literacy organizations to collaboratively create privacy tools, our study did not investigate specific learning techniques or particular content that works well with staff.

Third, **upgrading digital literacy curriculum to include privacy education requires that privacy protecting tools become easier to use**. End-user privacy protection should be available to all individuals—not just to "digital natives" or individuals with postgraduate degrees. Some researchers have suggested that engineers embed or "bake" privacy protection features into digital technologies, creating "privacy by default."[36] Products with these built-in privacy features would be one less worry for underserved populations as they turn to the Internet to take care of critical personal needs. When privacy protecting tools are as easy to use as seatbelts or sunscreen, classroom instruction will become easier too, lifting the burden on teachers to explain complex concepts to students in a short amount of time.

Fourth, from a larger broader perspective **it may be time to think about how to connect cybersecurity discussions with privacy debates**. In our study, we found that marginal Internet users talked about personal privacy and personal cybersecurity in the same breath. While some policymakers have spoken about the connection between cybersecurity and privacy,[37] the wider public discourse remains focused on national security versus personal liberty.[38] In light of the practical, everyday challenges presented here, there is a case to be made for addressing security and privacy problems together, in coordinated fashion. Such an effort could benefit not just marginal Internet users, but Internet users at large, and lead to a truly inclusive digital society.

Notes

[1] Chris Jay Hoofnagle and Nathan Good, *The Web Privacy Census*, October 2012, http://law.berkeley.edu/privacycensus.htm.

[2] *The Wall Street Journal*, "What They Know," 2010, http://blogs.wsj.com/wtk/.

[3] Pew Research Center, *Anonymity, Privacy, and Security Online*, September 5, 2013, http://pewinternet.org/Reports/2013/Anonymity-online.aspx.

[4] Jonathan Mayer, "Tracking the Trackers, Self-Help Tools," The Center for Internet & Society, September 13, 2011, https://cyberlaw.stanford.edu/blog/2011/09/tracking-trackers-self-help-tools.

[5] Leslie K. John, Alessandro Acquisti, and George Loewenstein, "Strangers on a plane: Context-dependent willingness to divulge personal information," *Journal of Consumer Research* 37, no. 5 (2011): 858-873.

[6] Pew Research Center, *Who's Not Online and Why*, September 25, 2013, http://pewinternet.org/Reports/2013/Non-internet-users.aspx.

[7] The NTIA supplemental survey contained nearly 50 questions.

[8] John B. Horrigan, "Broadband Adoption and Use in America," Federal Communications Commission Omnibus Broadband Initiative Working Paper Series, 1, February, 2010, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296442A1.pdf.

[9] Horrigan, "Broadband Adoption and Use in America." The same survey also found that non-adopters—individuals who do not subscribe to a broadband service at home—feel that it is easy to have one's personal information stolen online).

[10] Joseph Turow, "Audience construction and culture production: Marketing surveillance in the digital age," *Annals of the American Academy of Political and Social Science* 597 (2005): 103-121.

[11] Seeta Peña Gangadharan, "Digital inclusion and data profiling," *First Monday* 17 (2012): 5.

[12] Latanya Sweeney, "Discrimination in online ad delivery" *Social Science Research Network* (January 28, 2013), http://dx.doi.org/10.2139/ssrn.2208240. See also Safiya Umoja Noble, *Searching for Black Girls: Ranking Race and Gender in Commercial Search Engines*, (Ph.D. dissertation, University of Illinois, Urbana-Champaign, 2011).

[13] Joseph Jerome, "Buying and Selling Privacy: Big Data's Different Burdens and Benefits," *Stanford Law Review* 77 (2013), http://www.stanfordlawreview.org/online/privacy-and-big-data/buying-and-selling-privacy.

[14] Spencer Ackerman, "FBI Crime Maps Now 'Pinpoint' Average Muslims," *Wired*, October 24, 2011, http://www.wired.com/dangerroom/2011/10/fbi-geomaps-muslims/.

[15] Michelle Alexander, "Breaking My Silence," *The Nation*, September 4, 2013, http://www.thenation.com/article/176030/breaking-my-silence# Also: Andrew O'Hehir, "The NSA-DEA Police State Tango," *Salon*, August 10, 2013, http://www.salon.com/2013/08/10/the_nsa_dea_police_state_tango/.

[16] Peter Micek, "A Genealogy of Home Visits: Explaining the Relentless Search for Individualized Information Without Individual Suspicion," University of San Francisco Law Review, 44 (2010): 1007-1032. Virginia Eubanks, *Digital Dead End: Fighting for Social Justice in the Information Age*, (Cambridge, MA, MIT Press, 2011).

[17] The current study forms part of the Open Technology Institute's broader work on privacy and security—work that spans innovations in privacy protecting tools, policy analysis, and applied research. The author is also a visiting fellow at the Yale Information Society Project, where the study was originally conceived.

[18] Originally, the researcher invited six groups of varying sizes and missions. One group declined the invitation. Another agreed to participate, but later ceased operations. The remaining four organizations varied in audiences served and digital inclusion focus.

[19] Sizes of staff working on digital literacy ranged from five to nearly forty.

[20] The organization could provide its own list of popular websites or opt to share log files, through the temporary set-up of a proxy server that anonymously collected Web traffic.

[21] Eubanks, *Digital Dead End*.

[22] Each organization decided upon a unique process to codesign the learning tool.

[23] Work with the library system involved observation of drop-in introductory Internet and computer classes with a total of 11 students (a majority Latino immigrant women); engaging in a collaborative process to create a set of privacy literacy handouts that included six group discussions with a total of nearly 80 staff, and eight curriculum design meetings with 10 staff; and accessing a list of the 100 most popular websites visited in a single month at library system terminals. Note that most of the urls were unusable, however, because they pointed to ad networks or third party content.

Work with the citywide computer training center involved observation of 12 classes (two-thirds male, mostly African Americans, with one immigrant man of African descent); engaging in a collaborative process to create a learning tool that included five group discussions with 6 staff to build lesson plans on privacy and safety, and one group discussion with 12 students; and accessing a list of 100 most popular websites visited in a single month from a single terminal.

Work with the social movement organization entailed observation of four classes (featuring a diverse mixture of racial and ethnic backgrounds, ages, and gender); engaging in a collaborative process to create a learning tool, including one group discussion with 2 staff; and accessing a short list of (seven) websites recommended to program participants. Though the group wished to produce a learning tool, time did not permit completing this tool prior to the writing of this report.

Work with the senior center involved one activity: engaging in a collaborative process to create a learning tool. A total of four discussions took place with 12 staff members. Because the group elected to create a conversation guide (as opposed to class curriculum) as its learning tool, the process also entailed one-on-one interviews with 3 volunteer digital literacy trainers, 2 staff members, and 4 senior citizens (one of South Asian descent, the others African American).

[24] Gangadharan, "Digital Inclusion and Data Profiling." O.H. Gandy, *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage*, (Burlington, VT, Ashgate, 2009).

[25] See http://www.netograph.com.

[26] For more details, see Dharma Dailey, et al., *Broadband Adoption in Low-income Communities*, (Brooklyn, NY, Social Science Research Council, 2010). Also E-Government Act, 2002, Public Law 107–

347, 107th Congress, 2nd session, (December 17, 2002), http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[27] John Gilliom, *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*, (Chicago, University of Chicago Press, 2001). Eubanks, *Digital Dead End*.

[28] Seeta Peña Gangadharan, Kayshin Chan, and Kistine Carolan, *The Keyspot Model: A Home away from Home*, (Washington, DC, New America Foundation, 2013).

[29] Pew Research Center, "*Partisan Polarization Surges in Bush, Obama Years: Trends in American Values: 1987-2012*," June 4, 2012, 61, http://www.people-press.org/2012/06/04/section-5-values-about-business-wall-street-and-labor/.

[30] Nate Silver, "Public Opinion Shifts on Security-Liberty Balance," 538 Blog, posted July 10, 2013, http://fivethirtyeight.blogs.nytimes.com/2013/07/10/public-opinion-shifts-on-security-liberty-balance/?_r=0.

[31] Most study participants were public Internet adopters, rather than nonusers. So this finding is unsurprising.

[32] Samantha Becker, et al., *Opportunity for All: How the American Public Benefits from Internet Access at U.S. Libraries* (Washington, DC, Institute of Museum and Library Services, 2010).

[33] See http://www.youradchoices.com/. Also http://www.iab.net/privacymatters/.

[34] Pew, *Anonymity, Privacy, and Security Online.* This study erroneously targets use of a public computer as a means of "invisibilizing" one's digital footprint. In fact, a user could browse anonymously, but if she were logged into Facebook or another user account, her anonymity would cease. As user name registration has become the norm across the Web, the validity of a response option focused on public Internet browsing is tenuous.

[35] The situation recalls a well-known Web-based comic strip by XKCD that explains how humans have a hard time with remembering passwords that are easy for computers to guess. See https://xkcd.com/936/.

[36] Ira S. Rubenstein and Nathan Good, "Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents," *NYU School of Law, Public Law Research, Paper No. 12-43* (August 11, 2012), http://dx.doi.org/10.2139/ssrn.2128146.

[37] In Congressional testimony, Jason Weinstein said: "American who are using infected computers and mobile devices are suffering from an extensive, pervasive invasion of their privacy at the hands of these criminals almost every single time they turn on their computers." Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcommittee on Privacy, Technology and the Law of the Senate Committee on Judiciary, 112th Congress (2011) (statement of Jason Weinstein, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice), http://www.senate.gov/fplayers/CommPlayer/commFlashPlayer.cfm?fn=judiciary051011&st=xxx).

[38] Silver, "Public Opinion Shifts on Security-Liberty Balance."

MAIN OFFICE
1899 L Street, NW
Suite 400
Washington, DC 20036
Phone 202 986 2700
Fax 202 986 3696

NEW AMERICA NYC
199 Lafayette St.
Suite 3B
New York, NY 10012

NEW AMERICA FOUNDATION

WWW.NEWAMERICA.NET