Virtually Unused

Virtual Private Networks and Public Internet Users

Seeta Gangadharan, Bryan Dosono, Kitior Ngu, Open Technology Institute*

November 2013

How accessible is privacy and security software? Though recent research and news reports find that Internet users are taking measures to secure themselves online, a short survey completed by the Open Technology Institute (OTI) at New America Foundation suggests that public library Internet users may not be as nimble. Looking at Virtual Private Networks (VPNs), OTI found that almost none of nearly two hundred public library Internet users took advantage of this particular tool, and only eight individuals even knew what a VPN was. A majority of these respondents are library "dependents," meaning they have no alternative means of access to the Internet, and most engage in online transactions that require they input personal data like credit card information, bank account number, Social Security number, or birthdate. Meanwhile, the press and public agencies, like the Federal Trade Commission's OnGuardOnline.gov website, routinely advise public Internet users to refrain from such online activities unless subscribing to VPN services. Clearly the message and resources are not getting from VPN advocates to these users. Until new policies and practices focus on accessible solutions that apply to all individuals wanting to go online, security and privacy risks fall disproportionately upon certain kinds of Internet users.

As concerns for personal privacy and security in digital contexts increase,[1] a range of new tools have become widely available, making it possible for end users to manage and control their digital footprints. These tools have a range of purposes, from securing personally sensitive transactions to signaling to advertisers to refrain from tracking one's online behavior to anonymizing one's Internet activities altogether.[2] A number of educational resources have also cropped up in recent years, with the aim of shaping users' behavior to engage in safer practices online.[3] Meanwhile, adoption of such tools and resources among average Internet users is modest, but increasing.[4]

But are these tools accessible to public Internet users—especially those who rely on public access

* *Seeta Peña Gangadharan is a Senior Research Fellow at the Open Technology Institute. Kitior Ngu is a doctoral candidate in Communication at University of Michigan, Ann Arbor. Bryan Dosono is a doctoral candidate in Information Science at Syracuse University.* *The authors would like to thank OTI colleagues and anonymous reviewers for their input and insights.*

to the Internet because they lack it at home?[5] Different from average users, these public Internet adopters typically hail from poorer communities and communities of color. Many of them are marginal Internet users, who are coming online for the first time and learning new digital literacy skills. Furthermore, as survey research has demonstrated, lower income Internet users more frequently contend with problems like identity theft and experience other harmful consequences related to information sharing.[6]

The following report tackles the above question by focusing on adoption rates of virtual private networks (VPNs) among public Internet users. From popular press to policymakers, security advice directs users to subscribe to VPNs as a way to protect their privacy when using public networks. But a survey completed by the New America Foundation's Open Technology Institute (OTI) found that almost none of the nearly two hundred respondents approached at public library branches, one of the most common sites of public Internet access, used a VPN or knew what it was. The results suggest that it is time to recalibrate privacy and security recommendations so that they meet the needs of all Internet users, including the poorest among them.

Background

Public libraries provide Internet access to the country's most underserved communities. According to a 2010 survey which queried approximately 48,000 respondents, researchers at the University of Washington estimated that members of a significant minority (nearly 44 percent) of households below the poverty line had accessed the Internet at a public library.[7] Researchers also found that the library was indispensible to some: approximately 16 million individuals accessed a public library computer in order to go online, and approximately 4 million used their own computer to access library WiFi, *in the absence of alternative means of access to the Internet*.[8] These library "dependents" demonstrated high volume usage as well. For those using wired connections, 43 percent of "dependents" used an Internet terminal every or most days of the week. For "dependents" using WiFi, that figure amounted to 26 percent. (By comparison, only 16 percent of respondents with alternative means of Internet access report daily or almost daily usage of library Internet terminals. That number decreases to 14 percent in the case of library WiFi.)

Like a handful of other studies,[9] the University of Washington study also showed that many library patrons used the Internet as a lifeline to perform vital tasks. Users frequent libraries to renew their eligibility in public welfare programs. They stay in touch with family. They apply for jobs. They prepare for General Education Development (GED) tests. Without a public library, many members of underserved communities would struggle in the face of not only a digital divide, but also social and economic divides.[10] Public Internet access matters to individuals and aids in their political, economic, social, and psychological well-being.

In this study, OTI takes a look at common security advice to public Internet users and examines it in the context of the public library. Our original research question arose when library staff members talked with us about public WiFi recommendations mentioned on the site, OnGuardOnline.gov.[11] The Federal Trade Commission (FTC) created this website as a go-to resource for Internet consumers to be "safe, secure and responsible online."[12] It instructs

users of public wireless networks to use VPNs when engaging in personally sensitive transactions online. In the absence of protective measures, OnGuardOnline advises the public WiFi user to refrain from conducting personally sensitive transactions.

In reviewing OnGuardOnline, we recognized that the site offers a suite of recommendations—not just VPN adoption—when talking about safety on public WiFi. For example, the site recommends individuals check that they are on a WPA2-secured connection, which affords greater security than other kinds wireless security standards. The site also advises individuals to use secure HTTPS connections and to have different, strong passwords for different user accounts. Due to constraints of time we elected to focus on VPNs only and save a comprehensive review of security practices of public Internet users for later. Apart from time constraints, we focused on VPNs due to the fact that proper use requires adequate knowledge of what VPNs do and protect. Conversely, improper use can give users a false sense of safety, putting them at greater risk.[13]

We examined other sources of security advice, as well, and found that OnGuardOnline echoes other popular recommendations from the press and technology companies. From DIY sites like *Lifehacker* to corporate behemoths like Microsoft, experts similarly instruct public Internet users (both wired and WiFi) to either use a VPN or avoid transmitting personal data.[14] These resources explain how traffic routes securely through a VPN and protects the user's data. Though some VPN subscriptions are free, most are not. Several security advice websites caution against transmitting highly personal data via free VPNs, such as Social Security numbers or health records, due to concerns about the quality or strength of these products.[15]

In researching VPNs, we also discovered that although VPN adoption is far from mainstream, it has a growing market and appeal, especially given recent news concerning the extent of government surveillance. Pew Research Center reported that 14 percent of (nearly 800) respondents reported having subscribed to a VPN or other services that help users cover their digital footprints.[16] Following Edward Snowden's NSA surveillance revelations, one VPN provider recently reported a major bump in subscriptions (more than 50 percent).[17] These studies suggest that both anonymity and security factor into reasons for which Internet users turn to VPNs.

Design

To examine the practicalities of VPN advice, we conducted a short survey in Washington, D.C., querying patrons of the local public libraries about VPN adoption. We visited 13 out of the 26 public library branches across the District, focusing on patrons who use the public computers within the libraries. The District's library system has witnessed an increase in the number and usage of its public computers, including for such activities as applying for jobs, filing for unemployment benefits, and communicating with teachers.[18] Specifically, we asked study participants if they used public computers at libraries for sensitive transactions, whether they protected their online transactions using a VPN, whether they sought information security advice from library staff, and whether they understood the purpose of VPN tools (see Appendix 1 for full list of survey questions).

Data Collection

We collected data over a three-day period through a paper-based survey. We purposefully selected library branches to cover a range of poor to affluent neighborhoods in the entire District and randomly solicited adult patrons exiting libraries to complete the survey.[20] We limited the demographic data collected to age, since age often appears to factor into differences in norms and practices regarding privacy and security online,[19] and since other variables that typically define underserved populations in D.C. are well established.[20] We did not collect any identifying information of survey respondents.[21]

Results

Data obtained from the fieldwork reveal a lack of awareness or familiarity with VPNs among D.C. residents who use public library Internet. Of the 189 surveys completed, only 4.2 percent (eight respondents) of the sample population expressed some familiarity with VPNs (See Appendix 3, Table 6), and these respondents were all under the age of 44. A negligible proportion of users (1.1 percent, two respondents) reported using VPNs on a regular basis, stating they used VPNs when conducting personally sensitive transactions online. Only ten participants (5.3 percent of the sample) responded "Yes" to the question, "Has the library staff ever talked to you about Internet security?" one of whom admitted only hearing it mentioned to others (See Appendix 3, Table 4).

The majority of public computer users did, however, utilize these computers to conduct personally sensitive transactions online: approximately three-quarters of survey respondents (74.1 percent, 140 participants) described such use (See Appendix 3, Table 2). The age groups most likely to conduct personally sensitive transactions online included the 25-34 and 35-44 categories, comprising more than 50 percent of the surveyed respondents who responded in the affirmative (See Appendix 3, Table 7).

Survey results also revealed a high number of users whose only access to a computer comes from the public library system. Just over half of the sample population (52.9%, 100 participants) were wholly dependent on the public libraries for computer access (Appendix 3, Table 5). Fifty-five percent of this "dependent" group used public computers to fill out personally sensitive information online (See Appendix 3, Table 8). Compared to younger age groups, participants aged 35 and older were more likely to depend on libraries for computer use. Nearly 70 percent of users in this category (81 participants in total) did not have access to a computer other than those located in the library (See Appendix 3, Table 9). It is also worth noting that *none of the respondents who rely solely on public computers were familiar with VPNs*. The eight participants who mentioned familiarity with VPNs stated they had access to other computers.

Discussion

Our findings suggest that online privacy and security may be a difficult goal to reach for the Internet's most vulnerable populations. According to our initial analysis, public library Internet users:

- depend on public library Internet and use public library computers to complete personally sensitive transactions, but
- do not use VPNs to protect themselves when conducting personally sensitive transactions,
- are unaware of VPNs or their purpose, and the few individuals who are familiar have alternative means to access the Internet, and

- almost never receive on-site security advice in the context of public library Internet access.

This state of affairs presents marginal Internet users with a conundrum. On the one hand, some government programs of the past (or nearly past, such as the Broadband Technology Opportunities Program), current (E-rate), or future (ConnectEd),[22] provide places like libraries with the funds for public Internet access and urge members of historically marginalized communities to go online at these community spaces in order to facilitate civic engagement, education, employment, and personal prosperity. On the other hand, other government programs, such as the FTC's main privacy education Web resource, OnGuardOnline, tell people that if they are unable to secure themselves effectively with end-user tools like VPNs that they should stay offline in order to protect themselves from unwanted surveillance and privacy intrusions.

This puts public library Internet users in a difficult place: either go online insecurely and risk being the target of malicious emails, phishing scams, harassment, and identity theft, or stay offline and risk losing public benefits, missing job opportunities, learning about and managing one's health, and more. Neither option presents users with a fair deal.

Some may ask whether public library Internet users face any greater risk than ordinary Internet users. Indeed harms from security breaches affect all types of individuals. But as already mentioned, research has shown that respondents living in households earning less than $30,000 reported a greater number of problems due to sharing personal information online.[23] Taken together with the fact that members of poorer households are more likely to rely on public Internet access, such as at libraries,[24] this suggests that public Internet users disproportionately feel the impact of the insecurities of Internet access.

Although our survey did not ask respondents whether they would pay for a VPN, the fact that a majority of users rely on Internet access at a public library suggests that cost issues may be in play. That is, although some privacy advocates argue that market solutions can reduce privacy invasions,[25] the case of the public library Internet user suggests otherwise: a dependency on a free network to perform vital activities may expose users to harms they cannot afford to prevent. Further research could help illuminate the extent to which VPN subscriptions are mismatched with the economic reality confronting such users.

Further research could also explore where public library Internet users obtain information and tools that help them be safe online. Our survey only asked about security advice from library staff members. But patrons may learn from watching the news, seeing products advertised in window displays at a local corner shop, or finding out from friends and family. Needless to say, it would be helpful to identify popular sources of security advice for the public Internet users in order to improve them or public education campaigns like OnGuardOnline.

Finally, a word on security of public WiFi versus wired connections. In our survey, we did not ask respondents to indicate whether they went online using their own device. This may have made our survey results less fine grained, but we speculate that the short length of the survey made it more inviting for respondents to consent and complete the survey.

Recommendations

What can we do to make online security more accessible?

The following list provides a set of recommendations designed to initiate conversation about possible practical solutions. The list sets forth ideas that relieve the burden on the individual end-user and demands greater responsibility of policymakers, tech developers, and intermediary organizations like public libraries that support public Internet users' access a vital communication resource.

First, the FTC should stop giving advice that potentially puts public Internet users—particularly those dependent upon public Internet access—in a quandary. These users should not have to choose between insecurity and lack of connectivity. Public Internet users should also not be led down a false path of safety. No one should use VPNs without adequate understanding of what this tool offers or what constitutes proper use. Just as some end users misinterpret tools like "Private Browsing Mode," VPN use could give public Internet users a false sense of safety.[26]

Instead, the FTC could consider proposing solutions for institutions that design and deploy public networks. The agency could transform its education campaigns to include tailored advice for providers of public Internet access, especially non-profit entities like public libraries and community anchor institutions committed to bridging the digital divide. A key component of its recommendations could focus on network design choices that make security a seamless part of end users' browsing experiences. For example, the FTC could advise public Internet providers to set up networks with WPA2 encryption or suggest they install tools like HTTPS Everywhere and NoScript, which make Internet browsing and transactions safer and more transparent.[27] In addition, the agency could advise public Internet providers to physically secure computer terminals, cable and USB ports, and related infrastructure that rogue actors could otherwise hijack.

Second, libraries could also implement point-of-use ways to educate patrons about online security and protective measures. For example, each computer should display a flash page when users log on that clearly spells out the risk of conducting sensitive transactions online, provides links to a range of resources, and displays the option to receive assistance from a librarian. More broadly, library staff could also improve their general knowledge and expertise about online security. Libraries could invest in trainings for personnel who work with patrons on the library floor and in digital literacy classes in order to make patrons aware of best security and privacy practices. These trainings could go beyond what is currently available, reaching frontline personnel, not just IT staff.[28]

Naturally, this requires resources and policy attention. Libraries have no shortage of motivation to protect their patrons' privacy. Patron privacy forms a core tenet of public library service.[29] But they do have a shortage of funding. In recent years, public libraries have witnessed dramatic cuts in budgets, translating into fewer resources to handle increased demand for library services, including Internet access.[30] The same budgetary constraints applies to other institutions that also provide public Internet access, especially to poorer communities.[31] Under these conditions, libraries find themselves unable to meet patrons' needs, security, privacy, or otherwise.

In light of this, federal agencies could do better in supporting services that help Internet users protect their privacy and security online. For example, The Federal Communication Commission's E-rate program could better prioritize VPN and other security services.[33] Although the program does include security software on its list of supported services, they fall under the "Priority 2" classification, and the program's limited budget results in the vast majority of "Priority 2" requests not receiving annual E-rate support.[34] As the Commission undertakes an extensive review and modernization of the E-rate program, it should more explicitly support services that protect school and library Internet users, including VPN services, and as a result integrate greater security into institutions' network planning and design. Ensuring that schools and libraries have adequate broadband capacity to meet the needs of their users is clearly a critical priority for the E-rate program. However, protecting users of those networks could also be considered as the program is reformed.

Lastly, we need bigger and better investments in security technologies that benefit public Internet users. Specifically, tech developers should have greater incentives to make products that relieve end users of the burden of securing their personal information. Some developers aim to develop security products with publicly accessible networks in mind. For example, developers at the non-profit Calyx Institute are working to bundle security products with Internet service, so that the end user does not have to worry about subscribing to a secondary service or downloading particular software by him or herself. This will make it possible for network managers at libraries, for example, to get connectivity that offers privacy and security tools by default.[35]

Currently, ventures like those at the Calyx Institute are the exception and not the norm. Creating the conditions—whether prizes, grant competitions, research funding, or similar mechanisms—to inspire the creation of quality products for public good will ensure that the promise of digital inclusion does not fall flat in the face of security challenges for the public Internet user.

Ultimately, all consumers—not just public Internet users—stand to benefit from technologies that make security easier. By focusing attention on security in public Internet contexts, policymakers, practitioners, and developers will bring a much needed improvement to the user experience of a population that disproportionately feels the effects of unwanted surveillance and intrusion online.[33] But when leaders in technology and public service begin to prioritize tools and resources that are accessible and usable, they signal to Internet users everywhere that personal cybersecurity is an important and achievable goal in today's digital society. No one should have to face security risks when careful planning, policies, and preparation can lead to effective safeguards and the prevention of harm.

Appendix

Appendix 1: Field Survey Questions

We administered a brief paper survey consisting of 6 close-ended questions (Yes/No responses). The survey, available in English only, asked participants the following questions:

1) Do you use the public computers in the Library? (YES/NO)
2) Have you ever used the computers to fill out personal information (such as your name, birthday or social security number) on a website or for other secure transactions such as banking or shopping? (YES/NO)
3) Do you use a Virtual Private Network when you log onto the computers? (YES/NO)
4) Has the Library Staff ever talked to you about Internet Security? (YES/NO)
5) Other than the library, do you have access to a computer? (YES/NO)
6) Do you know what a Virtual Private Network is? (YES/NO)

Demographic question asking their age range (18-24, 25-34, 35-44, 45-54, 55-64, 65+)

Appendix 2: Screen Shot of Tips for Using Public WiFi Networks as provided by OnGuardOnline.gov

Protect Yourself When Using Public Wi-Fi

So what can you do to protect your information? Here are a few tips:

- When using a Wi-Fi hotspot, only log in or send personal information to websites that you know are fully encrypted. To be secure, your entire visit to each site should be encrypted – from the time you log in to the site until you log out. If you think you're logged in to an encrypted site but find yourself on an unencrypted page, log out right away.
- Don't stay permanently signed in to accounts. When you've finished using an account, log out.
- Do not use the same password on different websites. It could give someone who gains access to **one** of your accounts access to **many** of your accounts.
- Many web browsers alert users who try to visit fraudulent websites or download malicious programs. Pay attention to these warnings, and keep your browser and security software up-to-date.
- If you regularly access online accounts through Wi-Fi hotspots, use a virtual private network (VPN). VPNs encrypt traffic between your computer and the internet, even on unsecured networks. You can obtain a personal VPN account from a VPN service provider. In addition, some organizations create VPNs to provide secure, remote access for their employees.
- Some Wi-Fi networks use encryption: **WEP** and **WPA** are the most common. WPA encryption protects your information against common hacking programs. WEP may not. WPA2 is the strongest. If you aren't certain that you are on a WPA network, use the same precautions as on an unsecured network.
- Installing browser add-ons or plug-ins can help, too. For example, Force-TLS and HTTPS-Everywhere are free Firefox add-ons that force the browser to use encryption on popular websites that usually aren't encrypted. They don't protect you on all websites – look for https in the URL to know a site is secure.

Appendix 3: Tables and Charts

Table 1. Libraries in District of Columbia surveyed in this study.

Libraries		
	Frequency	Percent
Capitol View	12	6.3
Deanwood	14	7.4
Dorothy I. Height	20	10.6
Georgetown	2	1.1
Lamond-Riggs	27	14.3
MLK Memorial	9	4.8
Petworth	14	7.4
South East	16	8.5
South West	12	6.3
Tenley Friendship	24	12.7
Watha T. Daniel Shaw	12	6.3
West End	18	9.5
Woodridge	9	4.8
Total	189	100

Table 2. Survey data responses from Question 2: Have you ever used the computers to fill out personal information (such as your name, birthday or social security number) on a website or for other secure transactions such as banking or shopping?

Fill Out Personal Information		
	Frequency	Percent
Yes	140	74.1
No	49	25.9
Total	189	100

Table 3. Survey data responses from Question 3: Do you use a Virtual Private Network when you log onto the computers?

Use a Virtual Private Network		
	Frequency	Percent
Yes	2	1.1
No	187	98.9
Total	189	100

Table 4. Survey data responses from Question 4: Has the Library Staff ever talked to you about Internet Security? (YES/NO)

Staff Mentioning Security		
	Frequency	Percent
Yes	10	5.3
No	179	94.7
Total	189	100

Table 5. Survey data responses from Question 5: Other than the library, do you have access to a computer?

Access to Other Computers		
	Frequency	Percent
Yes	89	47.1
No	100	52.9
Total	189	100

Table 6. Survey data responses from Question 6: Do you know what a Virtual Private Network is?

Familiarity with VPN		
	Frequency	Percent
Yes	8	4.2
No	181	95.8
Total	189	100

Table 7. Survey data from cross-tabulation between age and personal information

Age * Personal Information			
	Personal Information		
Age	Yes	No	Total
18-24	31	4	35
25-34	39	9	48
35-44	38	13	51
45-54	22	15	37
55-64	5	2	7
65+	5	6	11
Total	140	49	189

Table 8. Survey data from cross-tabulation between access and personal information

Access * Personal Information			
	Personal Information		
Access	Yes	No	Total
Yes	85	4	89
No	55	35	100
Total	140	49	189

Table 9. Survey data from cross-tabulation between age and access

Age * Personal Information			
	Access		
Age	Yes	No	Total
18-24	28	7	35
25-34	36	12	48
35-44	14	37	51
45-54	8	29	37
55-64	1	6	7
65+	2	9	11
Total	90	99	189

References

1 Pew Research Center, *Anonymity, Privacy, and Security Online*, September 5, 2013, http://pewinternet.org/Reports/2013/Anonymity-online.aspx. Survey results are based upon 792 respondents. Researchers weighted results to account for demographic discrepancies.

2 For example, HTTPS Everywhere, an open source tool created by the Electronic Frontier Foundation and the Tor Project, forces browser connections to a secure version of hypertext transfer protocol. See https://www.eff.org/https-everywhere. The Tor Project created Tor, through which users can communicate anonymously. Tor obscures a user's points of origin when she sends a message through the Tor network. See https://www.torproject.org.

3 Common Sense Media provides a series of educational tools designed for parents, children, and educators, focusing on mostly non-technical ways to detect and prevent insecure and unsafe behavior online. Most other educational tools focused on privacy literacy target children and parents.

4 Pew Research Center, *Anonymity, Privacy, and Security Online*. Michelle Singletary, "Identity theft's youngest victims," *Washington Post*, December 4, 2012, http://articles.washingtonpost.com/2012-12-04/business/35624964_1_identity-fraud-identity-theft-assistance-center-identity-thieves.

5 The Federal Communications Commission and U.S. Department of Commerce's National Telecommunications & Information Administration define such users as "non-adopters." We do not use this term throughout this paper, since we wish to avoid confusion when talking about adoption and Virtual Private Networks (VPNs) or other security tools, and we feel that the term does not adequately define the status of public Internet users who, for example, depend daily on libraries and other institutions to go online. See also, Pew Research Center, *Who's Not Online and Why*, September 25, 2013, http://pewinternet.org/Reports/2013/Non-internet-users.aspx.

6 Pew Research Center, *Anonymity, Privacy, and Security Online*.

7 Samantha Becker, Michael Crandall, Karen E. Fisher, Bo Kinny, Carol Landry, and Anita Rocha, *Opportunity for all: How the American public benefits from Internet access at U.S. Libraries* (IMLS-2010-RES-01), Institute of Museum and Library Services, Washington, D.C., 2010, http://www.imls.gov/assets/1/assetmanager/opportunityforall.pdf. Researchers surveyed nearly 48,000 individuals by phone and Web. Researches weighted results for known demographic discrepancies. Also, Kathryn Zickuhr, Lee Rainie, and Kristen Purcell, "Library Services in the Digital Age," Pew Internet & American Life Project, http://libraries.pewinternet.org/2013/01/22/library-services.

8 Becker, et al., *Opportunity for All.* See Appendix 3, Tables 6 and 7.

9 Seeta Peña Gangadharan, Kayshin Chan, and Kistine Carolan, *The KEYSPOT Model: A Home Away from Home*, Open Technology Institute, New America Foundation 2013, http://www.newamerica.net.

10 Amy Bach, Gwen Shaffer, and Todd Wolfson, "Digital Human Capital: Developing a Framework for Understanding the Economic Impact of Digital Exclusion in Low-Income Communities," *Journal of Information Policy* 3 (2013). Colin Rhinesmith, "Free Library Hot Spots: Supporting Broadband Adoption in Philadelphia's Low-Income Communities," in "Broadband Adoption," ed. Seeta Peña Gangadharan and Greta Byrum, special section, *International Journal of Communication* 6 (October 2012); Dharma Dailey, Amelia Bryne, Alison Powell, Joe Karaganis, and Jaewong Chung, *Broadband Adoption in Low-Income Communities*, New York, Social Science Research Council, 2010.

11 Specifically, the research arose when the lead author was codesigning a privacy literacy tool at a public library. Library staff members discovered the OnGuardOnline resource and then balked at the FTC's advice that users refrain from personal transactions if they're unable to use a VPN. See also Seeta Peña Gangadharan, *Joining the Surveillance Society?* Open Technology Institute, New America Foundation, September 30, 2013, http://newamerica.net/publications/policy/joining_the_surveillance_society.

12 The site forms part of a larger campaign called Stop, Think, Connect, which aims to "raise awareness among the American public about the need to strengthen cybersecurity and to generate and communicate new approaches to help Americans increase their safety and security online." See http://www.onguardonline.gov/stop-think-connect. The website has been highly regarded. In recognition of its usability and design, OnGuardOnline received an award of distinction from the Center for Plain Language. See http://centerforplainlanguage.org/awards/clearmark2012/.

13 For example, VPNs only provide truly secure access to digital resources stored on the same network as the end point.

14 Jordan Fried, "Why 2013 is the year you start using a VPN," *Lifehack*, August 15, 2013. http://www.lifehack.org/articles/technology/why-2013-the-year-you-start-using-vpn.html. Alan Henry, "Why You Should Start Using a VPN (and How to Choose the Best One for Your Needs)," *Lifehacker*, September 5, 2012. http://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs. "Five tips for using a public computer," *Microsoft*, www.microsoft.com/security/online-privacy/public-pc.aspx. Becky Worley, "Is it safe to bank on public WiFi? How not to get hacked!" *Yahoo News*, February 8, 2012, http://news.yahoo.com/blogs/upgrade-your-life/banking-online-not-hacked-182159934.html. Larry Seltzer, "Open public WiFi. How to stay safe," *Information Week*, March 1, 2013, http://www.informationweek.com/personal-tech/wireless/open-public-WiFi-how-to-stay-safe/240149727. "VPNs: What they do, how they work, and why you're dumb for not using one," *Gizmodo*, March 26, 2013.

15 Samara Lynn and Fahmida Y. Rashid, "The best free VPN clients," *PC Mag*, January 15, 2013, http://www.pcmag.com/article2/0,2817,2390381,00.asp.

16 Pew Research Center, *Anonymity, Privacy, and Security Online*.

17 Douglas Crawford, "NSA Prism revelations cause big jump in VPN use," *Best VPN. The VPN Authority*, August 27, 2013, https://www.bestvpn.com/blog/7364/nsa-prism-revelations-cause-big-jump-vpn-use/.

18 Aaron Weiner, "Off the books," *Washington City Paper*, February 27, 2013, http://www.washingtoncitypaper.com/blogs/housingcomplex/2013/02/27/off-the-books/.

19 danah boyd, *Why youth (heart) social network sites: The role of networked publics in teenage social life*, Berkman Center for the Internet, Cambridge, MA, (2009). See also, Helen Nissenbaum, "A contextual approach to privacy online," *Daedalus* 140, no 4 (2011): 32-48.

20 Income, Poverty, and Health Insurance Coverage in the United States: 2011, United States Census Bureau, http://www.census.gov/prod/2012pubs/p60-243.pdf. See also http://www.neighborhoodinfodc.org/nclusters/nclusters.html.

21 In the process of doing fieldwork, we confronted a few challenges regarding data collection. First, because the surveying took place during regular business hours in sweltering summer weather, many prospective respondents opted to rush into the air-conditioned libraries instead of answering questions outdoors; soliciting for survey responses was not permitted inside the libraries. Second, some prospective

survey respondents assumed that we were affiliated with government entities and declined to comment on their library use, presumably because of a distrust of government. Third, some study participants provided information well beyond the scope of the survey, sometimes launching into monologue (and thus preventing the research team from approaching additional study participants). For example, some participants noted that the public computers did not provide a privacy disclaimer when patrons log on. Study participants complained about time limits of public computers. Finally, we also suspect that we observed some potential social desirability effect at play: when queried about Internet uses, many study participants focused on filling out job applications or on other activities deemed socially acceptable.

22 See http://www.ntia.doc.gov/category/broadband-technology-opportunities-program, https://www.fcc.gov/encyclopedia/e-rate-schools-libraries-usf-program, and http://www.whitehouse.gov/the-press-office/2013/06/06/president-obama-unveils-connected-initiative-bring-america-s-students-di.

23 Pew Research Center, *Anonymity, Privacy, and Security Online*.

24 Pew Research Center, *Who's Not Online and Why*. Becker, et al., *Opportunity for All*. See also John B. Horrigan, "Broadband Adoption and Use in America," Federal Communications Commission Omnibus Broadband Initiative Working Paper Series, 1, February, 2010.

25 Kenneth C. Laudon, "Markets and Privacy," *Association for Computing Machinery. Communications of the ACM* 9, no 6 (September 1996): 104, http://www.eecs.harvard.edu/cs199r/readings/laudon.pdf.

26 See Jonathan Mayer, "Tracking the trackers: Self-help tools," *Center for Internet and Society*, September 13, 2011, https://cyberlaw.stanford.edu/blog/2011/09/tracking-trackers-self-help-tools.

27 See https://www.eff.org/https-everywhere and http://noscript.net/. Regarding WPA2 encryption, see http://blogs.cisco.com/smallbusiness/understanding-the-difference-between-wireless-encryption-protocols/.

28 Security trainings for libraries do happen already. See, for example, http://nlc.nebraska.gov/NCompassLive/. However, trainings could happen more widely, touching a wider range of staff members (beyond library IT staff), and more frequently.

29 American Library Association, An Interpretation of the Library Bill of Rights, September 19, 2002, http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.

30 See http://www.ala.org/advocacy/libfunding/public. Also, Marilyn Johnson, "U.S. public libraries: We lose them at our peril," *Los Angeles Times*, July 6, 2010, http://articles.latimes.com/2010/jul/06/opinion/la-oe-johnson-libraries-20100706. See also Weiner, "Off the books."

31 Broadband Technology Opportunities Program, a federal program that funds public computer centers, was supported by the American Reinvestment and Recovery Act of 2009. Congress has not allocated additional funding for the program. This could lead to the closure of thousands of public computer centers.

32 See *News Brief, Commitments for Funding Years 2012 and 2013*, Universal Service Administration Company, Washington, DC, October 11, 2013 http://usac.org/sl/tools/news-briefs/preview.aspx?id=510. Also, *In the Matter of Schools and Libraries Universal Service Support Mechanism, CC Docket No. 02-6, Estimate of Demand for Funding Year 2013*, Universal Service Administration Company, Washington, DC, April 22, 2013, http://www.usac.org/_res/documents/sl/pdf/tools/news/FY2013-Demand-Estimate.pdf.

33 Modernizing the E-rate Program for Schools and Libraries, WC Docket No. 13-184, Notice of Proposed Rulemaking, FCC 13-100, ¶ 1 (2013).
34 Disclosure: The director of the Open Technology Institute, Sascha Meinrath, sits on an advisory panel for the Calyx Institute, a not-for-profit organization. Calyx develops and advances free, open source end-to-end encryption, and to educate the public about approaches and methods to ensure privacy, free speech.
35 See also Gangadharan, *Joining the Surveillance Society?*

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