ACORN Canada's Protect Your Privacy-Online! Educational Program:

An Evaluation Report Prepared for ACORN Canada

By

Sherry Breshears, PhD Candidate, Faculty of Education, Simon Fraser University[i]

Dr. Suzanne Smythe, Assistant Professor, Faculty of Education, Simon Fraser University[ii]

March 31, 2017

Executive Summary

This evaluation reports on the outcomes of ACORN Canada's *Protect Your Privacy-Online!* project, funded by the Office of the Privacy Commissioner of Canada. This project consists of three workshops, offered in four Canadian cities and is designed to educate lower income Canadians about the Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA is Canada's Federal legislation that establishes rules for how private-sector organizations must protect the online privacy of Canadians. The Act also has implications for the education of citizens about their privacy rights, and about how they can protect their privacy online. *Protect Your Privacy-Online!* is one of the first community-based education projects in Canada to address the unique online privacy literacy needs of low income Canadians and to systematically address the skills and strategies available to citizens to protect their privacy in online environments.

The goals of the workshops were a) to expand participants' knowledge of PIPEDA; b) to introduce the scope of risks to one's privacy online; and, c) to provide strategies for protection against privacy threats. These goals are ultimately oriented to building participants' confidence to engage in digital participation, recognizing that safe use of the Internet is a valuable, even essential, practice of engaged citizenship and digital and social equity.

A review of literature provided in this report suggests that income and age are highly correlated with threats to privacy through Internet scams, phishing and hacking. This makes initiatives such as *Protect Your Privacy-Online!* all the more important. These themes emerge again in the findings of a background survey that explored digital access and education needs, and in the workshop evaluation. The background survey results indicate that while knowledge about online privacy is weak, people are intensely interested in the topic. The surveys also reveal the effects of Internet affordability on online participation and also point to powerful effects of income and age on confidence to use the Internet. Participants seemed to appreciate access to digital education opportunities that are timely, relevant and ongoing. People made suggestions for workshop design and delivery that combine principles of clear language, experiential and hands-on learning with their own devices when possible, and one-to-one support as well as small group learning.

In conclusion, *Protect Your Privacy-Online!* is a unique pioneering initiative that has supported the digital education of low income citizens in this vital and often neglected area. The workshops were very well received by communities, and the project has opened new sources of information and insight about the relationship between digital equity and the protection of privacy online. Indeed, low income and older citizens seem particularly vulnerable to breaches and threats to online privacy. This implies that efforts to enhance and protect online privacy and security should be located within policies that promote equitable access to the Internet, to devices that can be updated to the latest privacy settings, and to ongoing education opportunities such as *Protect your Privacy – Online!* These initiatives should attend to the intersections of technological change, new threats to privacy, social values, and the vulnerabilities of low-income citizens on the margins of digital access.

1. About the project

ACORN's *Protect Your Privacy-Online!* project, funded by the Office of the Privacy Commissioner of Canada, educates lower income Canadians about the Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA is Canada's Federal legislation that establishes rules for how private-sector organizations must protect the online privacy of Canadians. The Act also has implications for the education of citizens about their privacy rights, and about how they can protect their privacy online.

   Protect Your Privacy-Online! is one of the first community-based education projects in Canada to address the unique online privacy literacy needs of low income Canadians and to systematically address the skills and strategies available to citizens to protect their privacy in online environments. As new technologies proliferate, so do new forms of surveillance, information sharing, and information theft that are introduced by way of algorithmic tracking, hacking, phishing, video and audio file sharing and so on. This means that the need for educational interventions such as ACORN's PIPEDA workshops has become even more important. Indeed, older and low income Canadians who do not have regular access to a device that they own, who rely upon public Internet services, or who do not have access to digital skills training and secure servers through workplaces and higher education are more vulnerable to privacy breeches, Internet scams, phishing and hacking. As an anti-poverty organization that counts low income Canadians among its constituents, ACORN is well-placed to advance the educational goals of Internet security for these most vulnerable groups.

1b. Workshop content

The *Protect Your Privacy-Online!* project consisted of three workshops designed to be accessible for low-income participants from diverse language and literacy backgrounds. The goals of the workshops were a) to expand participants' knowledge of PIPEDA; b) introduce the scope of risks to one's privacy online; and, c) to provide strategies for protection against privacy threats. These goals were ultimately oriented to build participants' confidence to engage in digital participation, recognizing that safe use of the Internet is a valuable, even essential, practice of engaged citizenship and digital and social equity.

The first workshop was entitled "PIPEDA and You: Know Your Privacy Rights and Protect Your Info Online!" This workshop built participants' awareness of PIPEDA and the Office of the Privacy Commissioner's role in protecting their digital privacy rights. The workshop further enhanced participants' ability to identify possible privacy infringements by third parties, direct and file privacy complaints, and better protect sensitive information online and on their mobile devices. The lesson plan for "PIPEDA and You: Know Your Privacy Rights and Protect Your Info Online!" is provided in Appendix A.

The second workshop, "Digital Trails: Managing your Online Profile & Our Bodies as Information: Wearable Computing and Bodily Tracking Devices" consisted of two components. In Part 1, participants learned about "digital trails" and how their online activity has the potential to affect their personal and professional reputation. Participants explored strategies to manage their online profile responsibly. In Part 2, participants gained an appreciation of how the human body provides a wealth of intimate personal information that evolving technologies can exploit to compromise their privacy. This section of the workshop informed participants about how to identify and mitigate privacy security concerns resulting from wearable computing and bodily

4

tracking devices. The lesson plan for "Digital Trails: Managing your Online Profile & Our Bodies as Information: Wearable Computing and Bodily Tracking Devices" is provided in Appendix B.

The third workshop was "Personal Information as a Commodity: How the Private Sector uses Your Online Personal Information & Who is Watching You? Government Services and Surveillance Online." Part 1 of this workshop offered participants an understanding of how to better determine the privacy risks involved in participating in certain online activities including how private sector practices collect individuals' online information. Participants also learned about website terms and conditions and privacy policies. Part 2 of this workshop gave participants a broad overview of how government surveillance activities in Canada are carried out, the kinds of information gathered by government through these activities and how to use the Privacy Act to access personal information that the government may have collected. "Personal Information as a Commodity: How the Private Sector uses Your Online Personal Information & Who is Watching You? Government Services and Surveillance Online" is attached as Appendix C.

1c. Participant recruitment

ACORN Canada is a well-established anti-poverty advocacy organization that is membership-run. Members of ACORN include low-income Canadians from all walks of life: Seniors who rely upon CPP, older adults who rely upon income assistance, adults who work in low-wage sectors and people with disabilities. Participants for the PEPIDA workshops were recruited among the ACORN membership; email constitutes a barrier for some groups because they do not have Internet at home, and leaders knocked and doors and relied upon face to face invitations as part of their recruitment strategy. The charts provided in Part 4 note that most participants in the

workshops were over 40 years of age and either receive income assistance, are employed in the low wage sector or are retired.

2. Review of related literature: Digital inequality and online privacy

As noted above, the *ACORN Protect Your Privacy-Online!* project was one of the first in Canada to address the digital educational needs of low income Canadians with respect to privacy and security. The workshops unfolded in four regions across Canada in the context of prevailing digital inequalities that flow largely from income inequality and the unequal distribution of digital education opportunities across jurisdictions (ACORN Canada, 2015; CCPA, 2011). In this respect, maintaining online privacy and ensuring access to a secure Internet for all Canadians should be understood within the broader context of digital policy and efforts to address what many have called 'the digital divide' (Government of Canada, 2001). In this section, we briefly articulate the digital policy landscape internationally and within Canada, and identify the policy gaps and opportunities for enhancing online privacy and security; we then consider the scant literature that addresses the online privacy needs and barriers that low income groups and consider the unique contributions of PIPEDA and the ACORN *Protect Your Privacy – Online*! to this important and emergent work.

2b. The digital divide and online privacy

The Organization of Economic and Cooperative Development (OECD) has noted that the "first digital divide" between those who have access to computers and those who do not has "been effectively erased" (Burns & Novacs, 2014, para. 4) and argues that we are now in a second divide, one that shifts inequalities from technology access to technology use, in other words, "between individuals who have moved to embrace a technologically-rich world and those who

have been left behind" (Burns & Novacs, 2014, p. 4). The Government of Canada echoed this view in 2012 when it declared that the national Community Access Program (CAP), which funded community-based programs to offer public access to the Internet, to computers and to instruction, was no longer necessary because "the vast majority of Canadians are now connected to the Internet at home, while many more have access through their mobile devices" (Canadian Broadcasting Corporation, April 8, 2012). Underlying these pronouncements are two assumptions: First, that the digital divide is a technological issue that has been largely resolved with the spread of broadband access, and second, that persistent socio-economic inequalities are the result of a lack of skills among adults to cope in a technologically-rich world.

1c. Access and privacy: Internet affordability, access to devices, and digital education

Gilbert (2010) notes that digital divide research has remained largely at the descriptive, statistical level in terms of access and usage in ways that mask the complexities of digital access. In the results of the questionnaires gathered in the ACORN Workshops, this complex picture emerges. It becomes clear that digital access and the goals to protect the online privacy of low income Canadians need to be contextualized in three related factors: Internet affordability, access to well-maintained and newer devices, and access to timely and appropriate instruction. Yet Canadian digital policy does not adequately address these factors, tending to conceptualize digital access as an issue of infrastructure, the *potential* to access to an Internet connection. Moreover, in most national digital strategy documents, the goals of Internet access and digital education are described largely in terms of economic productivity and the potential efficiencies of digital government (cf. Industry Canada, 2015). Issues of personal privacy and secure access to the Internet are also under-represented in these documents.

Although *Digital Canada 150*, the most recent national digital strategy, acknowledges

that "affordability is a consideration" (Industry Canada, 2014b, para. 10), and a recent CRTC decision signals that access to the Internet should be considered a basic need, consumer and anti-poverty groups such as ACORN, have observed that there is little attention to how low and middle income Canadians will afford rising Internet and mobile data costs, nor how people will acquire and maintain digital devices (ACORN Canada, 2015; PIAC, 2015). Internet use is highly correlated to income: only 58% of households with incomes of $30,000 or less subscribe to the Internet (Statistics Canada, 2013). However, low income households reportedly sacrifice other basic needs to maintain an Internet connection. The Public Interest Advisory Committee (PIAC) study on digital access and government services found:

> [C]onsumers were reluctant to cancel their communications services, even in the face of increasing costs and tight household budgets […] Some consumers were even willing to cut other basic expenses, including food, clothing and health care, rather than cancel their communications services. Others insisted that they did not know where they could cut back in their household budget. (PIAC, March 2015, p. iv).

These interlocking issues of access have direct consequences for privacy and security of lower income Canadians. For example, in the results of the pre-workshop questionnaires carried out as part of the evaluation of the *Protect Your Privacy – Online!* project, respondents report that affordability of the Internet is a factor in their online participation. In addition, many people rely upon publicly available computers to carry out quite personal tasks related to e-government and banking, which introduces additional concerns for privacy and security. Access to well-maintained devices is also a concern because computers are designed for obsolescence within two to three years. Older devices are less reliable and less able to be updated to provide privacy and security. A third component of digital access and equity is education. Canadian digital policy

is also largely silent in this respect. Some municipal digital strategies indicate that computer education is available at public libraries, but there is little research that documents whether equitable and timely support to learn how to use the Internet and protect online privacy is available in all libraries in ways that meet local community needs.

2c. Internet privacy and safety: Challenges for low income Canadians

As noted above, there is little published research that considers the unique barriers to privacy and security online experienced by low income groups with precarious access to the Internet and digital resources. As Part 5 of this report indicates, the educational interventions offered by ACORN were well-received by the workshop participants. These workshops informed participants of their rights under PIPEDA, addressed the concept of personal responsibility for keeping one's identity and personal information secure, as well as managing one's online presence. This approach offers people a sense of control over their online activities. It also opens their awareness to the ways in which institutions and agencies online are fallible, subject to hacking and lapses in security protocol, and may also intentionally gather both personal and mega-data that can be used in identity theft.

A concern raised by scholars of digital equity is that education about online privacy and security might instigate mistrust of the Internet and dissuade people from online participation, further exacerbating digital inequalities because people are then excluded from the benefits of being online with respect to developing skills, participating in online society and finding resources (Haight, Quan-Haase and Corbett, 2014; Mossberger, Tolbert, & Franko, 2013). The PIPEDA curricular topics and the ACORN workshops thus offer a 'fine balance' between critical awareness of threats to privacy and ways to continue to benefit from what the Internet can offer.

2d. Privacy in a changing culture

These dynamics of digital access should also be read in the context of cultural and social changes regarding 'what counts' as privacy. Best (2010) has observed that personal and social values surrounding the ideals of privacy in a "networked world" are evolving alongside technologies and policies. She notes that people are often unaware of, or overwhelmed by, risks to online privacy, so that they may claim they have "nothing to hide" (p. 2). In addition, issues of consent that are so central to current privacy regimes are murky in the online world where forms of consent might be buried in dense and inaccessible legal texts, configured as 'opt out' so that people are not aware they have provided consent and so on. These are problems of individual literacy skills, but they are also problems of technology design, standards of 'informed consent' and enforcement.

Efforts to promote online privacy cannot rest with individuals alone. Online privacy protection will continue to be a shared responsibility, involving community-based vigilance and advocacy, policy development, and enforcement of privacy rights among commercial interests and social media conglomerates. The interests of low income Canadians must be integral to such frameworks. As Sloan and Warner (2014) observe, threats to personal privacy online are ever-evolving and "rapid technological developments have created novel situations that lack relevant norms" (p. 9). This suggests that efforts to enhance and protect online privacy and security should be located within policies that promote equitable access to the Internet, to devices that can be updated to the latest privacy settings, and to ongoing education that attends to the intersections of technological change, new threats to privacy, social values, and the vulnerabilities of low-income citizens on the margins of digital access to these changes. These themes emerge again in the sections that follow, which present findings of two surveys carried out among the workshop participants before and after their participation in the workshops.

3. Project activities, data sources and analysis

Protect Your Privacy-Online! consisted of a series of three 1.5-hour workshops offered in four cities: Toronto, Ottawa, Halifax and New Westminster, BC. Toronto and Ottawa each offered two separate workshop series for a total of six education interventions. The average attendance was more than ten, with a total of 66 participants. It is not known how many of these participants attended all three workshops.

At each of these workshops participants were invited to complete a pre-workshop questionnaire that addressed their digital skills and knowledge of Internet privacy, and, following the findings from the literature presented above, also explored dynamics of digital access including home Internet connections, ownership of devices, income and age. A sample of the questionnaire is provided in Appendix D. An analysis of the responses to these questionnaires is presented in Part 4 of this report.

Following the workshops, participants were invited to complete a workshop evaluation. This solicited feedback on the quality of the workshops, the new knowledge and skills about privacy participants felt they acquired, and suggestions for improvement. An example of this questionnaire is presented in Appendix E and the results are analyzed in Part 5 of this report.

4. Findings of the pre-workshop survey

The pre-workshop surveys were intended to assess aspects of workshop participants' digital access, digital literacy and knowledge of internet privacy. Here we summarize the responses quantitatively and cross-analyze the findings according to income and age where results differed

across these categories. Where appropriate, written comments are also quantified and sample comments are included to give depth and description to the analysis.

4a. Summary of responses to pre-workshop surveys

There were 66 responses to this questionnaire across four regions: British Columbia (15), Nova Scotia (4), Ottawa, Ontario (26), and Toronto, Ontario (21). Most respondents were over 40 years old (90%). 92% of respondents reported that English is the language they use most often in their daily lives and 78% have incomes less than 25,000 dollars a year (n=42). Of these, 55% said they receive government assistance.

Concerning digital access and affordability, the majority of respondents own a device (92%). We also noted, however, those without their own device were in the lowest income category (< $15,000 per year). Furthermore, while 65% reported having access to a private internet network, 17% rely solely on public internet service. We identified that this group of users may be particularly vulnerable to internet privacy breaches. In terms of internet affordability, 63%, or close to two-thirds, claimed that they either cannot afford the internet or they have to make sacrifices in order to be able to do so. This perception was true for respondents across income levels.

When asked about their digital skills, similar numbers of people reported having weak, average and strong skills (about 1/3 in each category). Age seems to play a considerable role in how respondents described their computer ability; level of computer skills and confidence in using a computer decreases along with the age of respondents. Those in the lowest income category (under 15,000 dollars per year) also tended to describe their skills as weak or average.

Similarly, 57% described their confidence using the computers safely as weak and 66% said their knowledge about protecting their privacy online was weak. Further to this, those in the

lowest income bracket were somewhat more likely to identify low confidence and knowledge of safety practices, and older adults were significantly more likely to report low confidence and knowledge of safety practices compared to younger people.

4b. Regional responses

As shown in the chart below, of the 66 completed pre-workshop questionnaires, 15 were from B.C., 26 were from Ottawa, Ontario, 21 were from Toronto, Ontario, and 4 were from Nova Scotia.

Number of pre-workshop surveys by region

Region	Number of surveys
BC	15
NS	4
Ottawa, ON	26
Toronto, ON	21
Grand Total	**66**

4c. Age

Of the 63 respondents who answered this question, only 6 (10%) were aged 40 or under, 16 (25%) were between 40 and 51, 28 (44%) were aged 51- 64, and 13 (21%) were older than 64.

Three people did not report their ages. This age group also traces the core membership of ACORN. We also note that among the respondents under 40, at least two live with their parents.
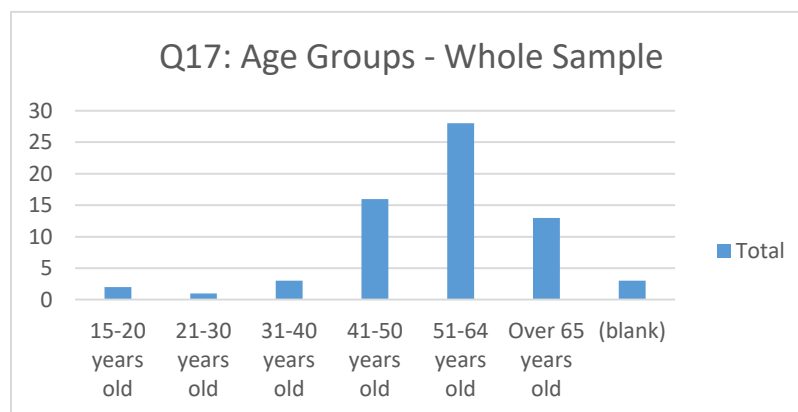
***Pre-workshop Survey* responses by age and region**

| Region	15-20 years	21-30 years	31-40 years	41-50 years	51-64 years	Over 65 years	Total (n=63)
BC	2		2	4	3	4	**15**
Nova Scotia				1	2		**3**
Ottawa, ON				7	10	7	**24**
Toronto, ON		1	1	4	13	2	**21**
Total	**2**	**1**	**3**	**16**	**28**	**13**	63
		(10%)		(25%)	(44%)	(21%)	

4d. Language

To the question, "What language do you speak most often?" 61 people (92%) answered

"English." Two people indicated that Arabic was the language they most often speak, and three

answered that French is their main language. When asked what languages they read and write

confidently, almost all respondents (61) said "English." Three indicated that they are most

confident reading and writing in French (5%), and one person did not respond.

Although English was indicated as the language in which people read and write most

confidently, when invited to offer written responses in the surveys, people demonstrated

orthographic and grammatical errors. In addition, comments were sometimes very short or left

blank, but the multiple-choice questions were answered more readily. In other cases, answers to

questions that were similar conflicted with one another, which could mean difficulties

understanding the questions due to language or literacy challenges.

**Q15: Written Language - Whole Sample**
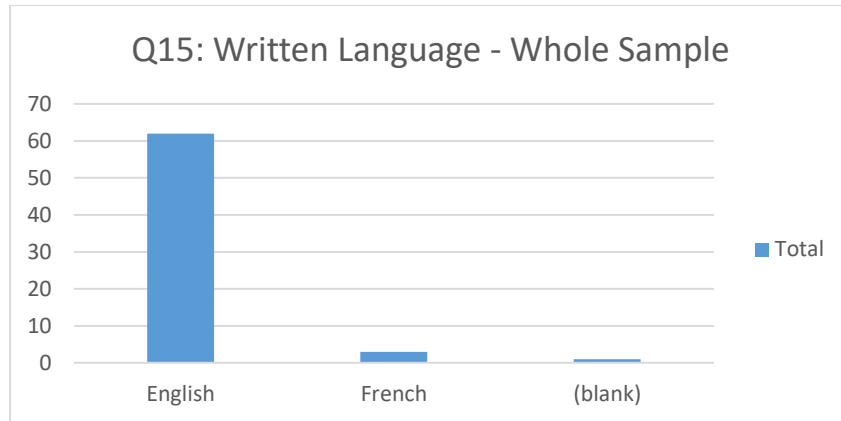
4e. Income

54 people responded to a multiple-choice question about their annual individual income. Of those, 31 (57%) reported an annual income of less than 15,000 dollars and 11 (20%) reported income between 16,000 and 25,000. In other words, about three-quarters (77%) of respondents have individual incomes of less than 25,000 dollars. Eleven people (20%) earn between 26,000 and 60,000 dollars a year, and only one reported earnings above 60,000.

Q18: Income
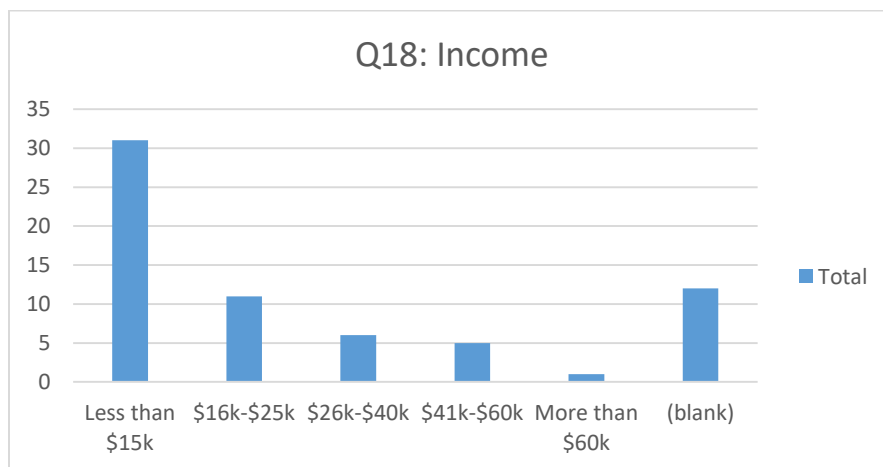
4f. Source of Income

Sixty people responded to the question about their main source of income. The primary response was government assistance, including income assistance or disability assistance (40%). The second most common answer was a pension plan, including Canada Pension Plan (33%).

Thirteen people (22%) people reported that full-time or part-time employment was their main source of income, and two people reported that they have no income at all. Of the 31 people who earn less than 15,000 dollars a year, 65% are on government assistance. Because income assistance eligibility is based on household income, we might interpret that most of these individuals live alone, or live with people who might also be considered as living on a low income.
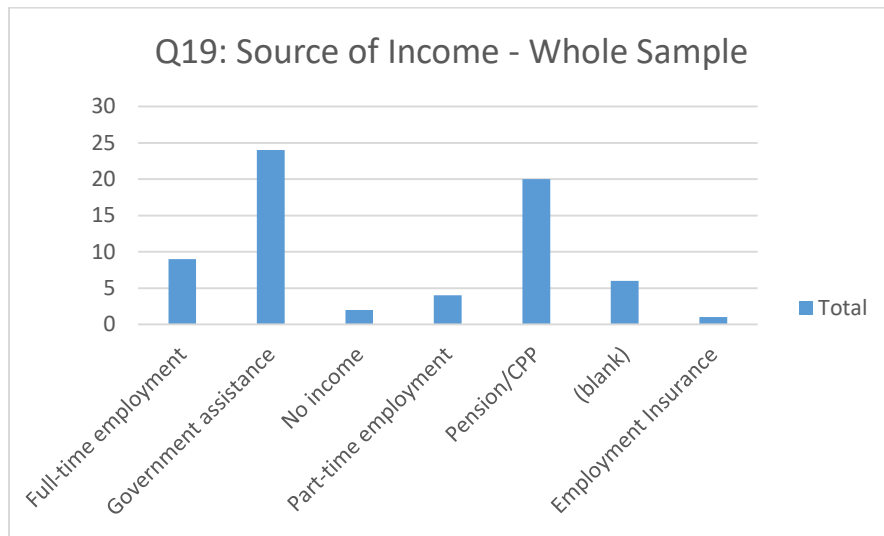

4g. Access to a Device

All but five people (about 8% of respondents) own a device. Notably, these five respondents reported annual individual incomes of less than 15,000 dollars. A number of respondents own more than one device. About half of respondents have access to a smart phone. The survey did not gather information about the age and functionality of the devices; this is often a factor in the capacity to update privacy settings, protect against viruses and phishing, and so on. The survey did not ask if the devices were purchased or donated, another important factor in gauging ongoing access to devices.

Q4: Owned Devices - Whole Sample
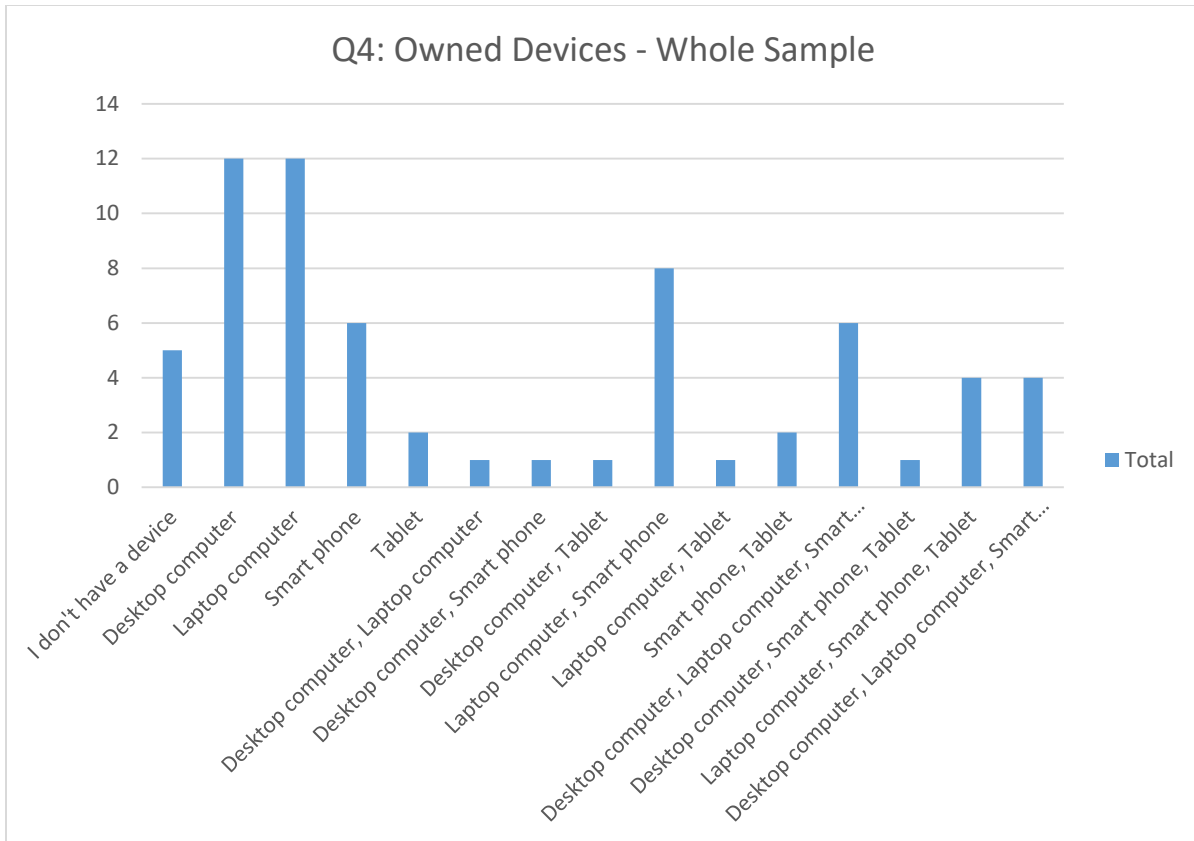
4h. Access to the Internet

65% of respondents access the Internet primarily from home on a private network (65%). Some users access the internet on a public network (17%), but very few access the internet through a data plan (3%). This is likely due to the high cost of data. Notably, 10 respondents (15%) report having no internet access at all.


Q7: Preferred Internet Access - Whole Sample
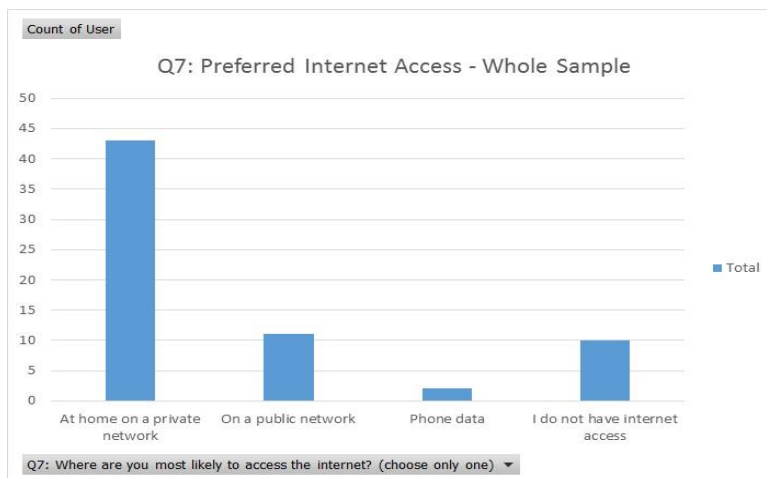
Laptops are the preferred device to access the Internet for those with incomes less than $15, 000, followed by smart phones. This reflects other research suggesting the decline of desktop computer use among all income levels.
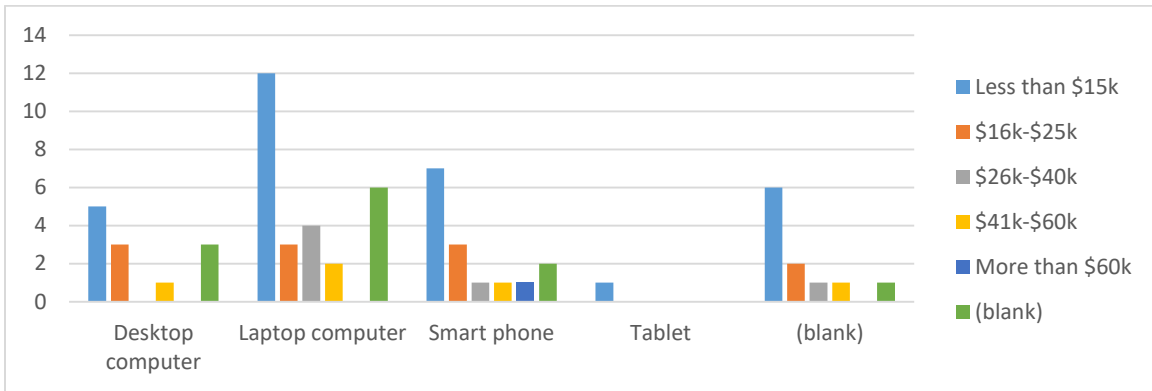

4i. Time spent on the internet

Research shows the more people use the Internet, the more likely they are to report confidence using the Internet and higher computer skills. Close to half of the respondents (45%) spend less than an hour a day on the Internet, while 28% spend up to 5 hours a day on the Internet. 27% of respondents report spending more than 5 hours a day on the internet. Since most (77%) of respondents in this sample earn less than $25,000, it is difficult to correlate Internet use with income in this survey. However, 76% of those reporting using the Internet less than once a day have incomes of less than $25,000.
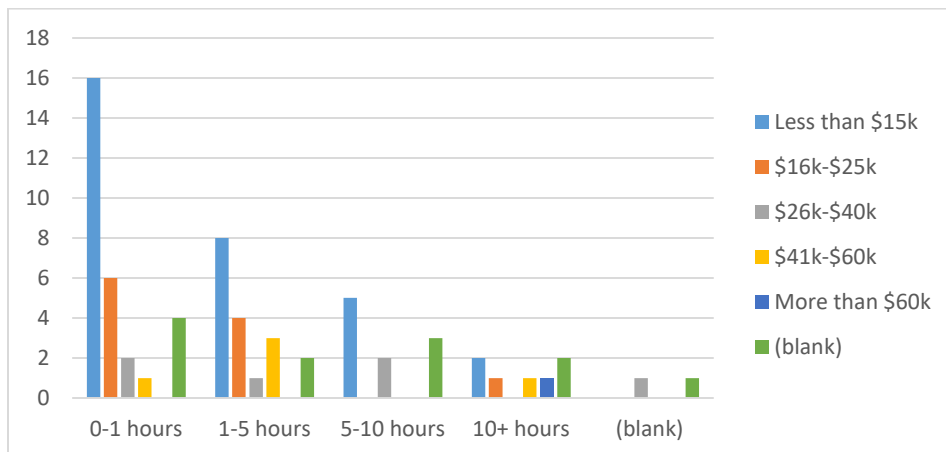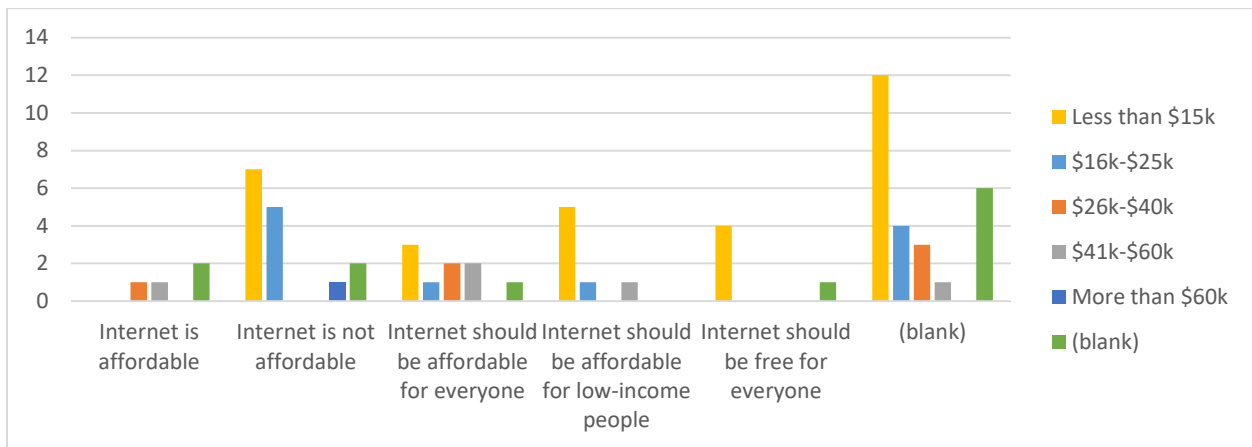
4j. Internet affordability

Respondents were asked about their experiences of Internet affordability. 48 responded to these questions and 12 said they did not know. Of those who expressed an opinion, 18 (37%) said they can afford it with their income. However, 22 (46%) said they make sacrifices in their budget to afford it, and 8 (17%) said they cannot afford Internet at home.
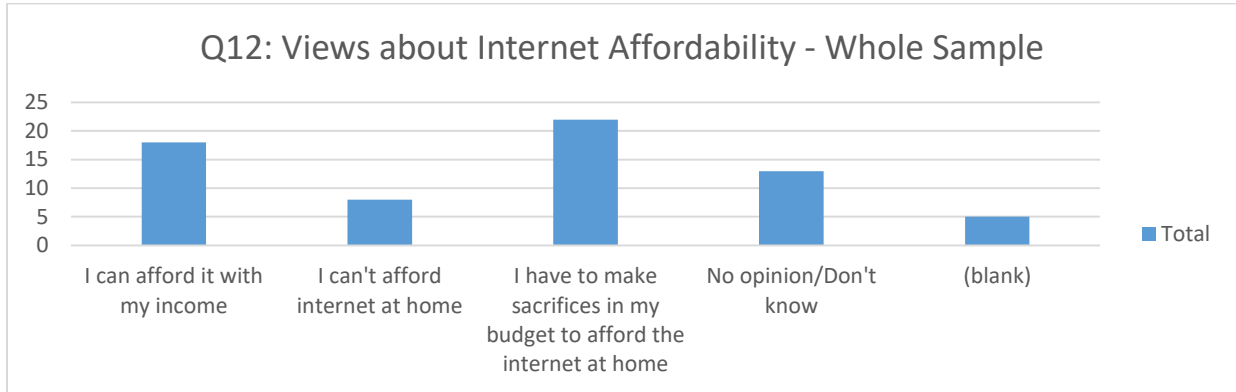
When asked to comment about their views on Internet affordability, only four people believe it is affordable. Fifteen people said they feel the internet is not affordable, and seven said that the internet should be affordable specifically for low-income people. Nine people said internet should be affordable for everyone, while five people feel the internet should be free for everyone.

When set against income level, people's views on affordability were consistent across income levels. Opinions about internet affordability are reflected in the following comments:

I feel it's a right and should be more affordable. (B.C.)

Too expensive to even buy one and pay for the monthly internet service. (B.C.)

I pay around $50 per month. (Ottawa)

It would be nice if it was $10/month. (Ottawa)

It is high and cheaper companies have less storage and slower speed of internet etc. (Toronto)

Many comments indicate that respondents feel their lives require them to access the internet on a regular basis, but it is not affordable for them to pay for home-based internet service.

Poor people are constantly being excluded from basic need as the internet is becoming more and more a way of life. It is part of our consciousness. (B.C.)

Fine if one is working. Otherwise not so much. (B.C.)

I have to make some sacrifices in order to have internet access because I need it too much in my daily life. (Ottawa)

I figure you need the internet now for finding a job, so now it is a necessity. (Ottawa)

Everything now you have to access the internet for. It should be affordable so that everyone can access it to do what is required of them. (Toronto)

4k. Computer skills

Respondents were asked how they would describe their skills using a computer. Of the 66 respondents, approximately one third (32%) said they are "confident," one third (36%) said they "get by" and another third (32%) said they are "struggling." Additionally, when respondents were asked to describe their computer skill level on a scale of one (weak) to five (strong), similar ratios appeared, with approximately a third selecting "weak" scores, a third in the middle, and a

third selecting "strong" scores. Notably, of the third who identified their skills as weak, most of these individuals (24%) felt their ability is very weak, with a score of one.
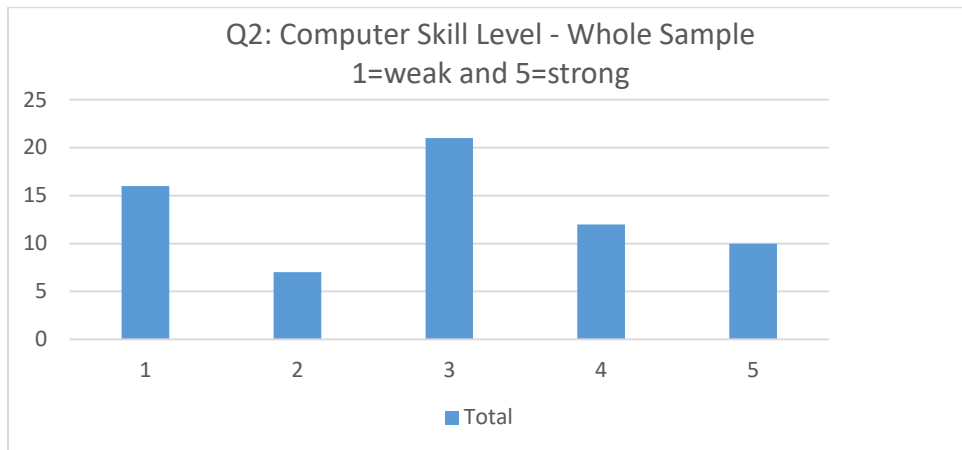

As suggested in the graphs below, people with reported incomes of less than $15,000 did not report significantly greater weakness than those with higher incomes. However, people with higher incomes reported somewhat higher levels of confidence.
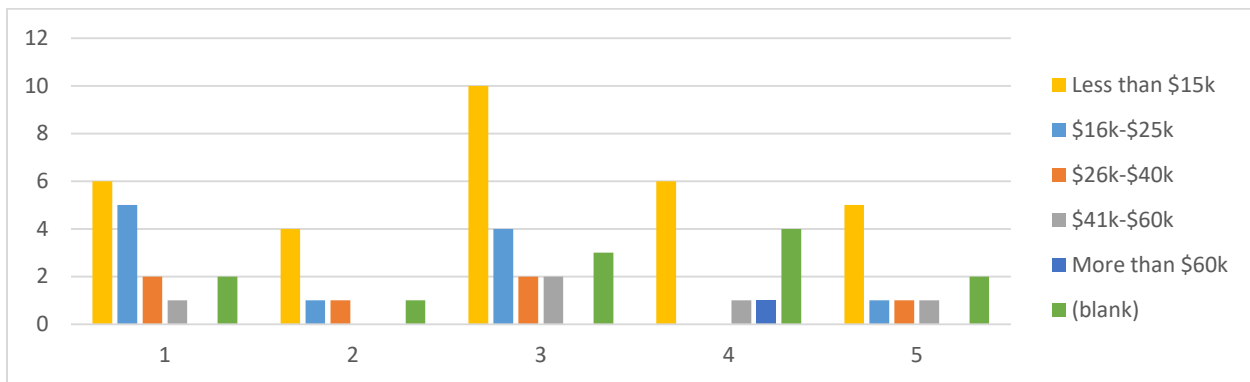
When digital skills and confidence are cross-analyzed with age, significant discrepancies appear. The older adults in the sample were more likely to see themselves as struggling or just getting by than the younger individuals. Of the 13 respondents that make up the oldest group, those who are more than 65 years old, eight respondents (62%), saw themselves as struggling. These results were echoed in the question where respondents were asked to select a number that describes their computer skill level, where 1=weak and 5=strong. Again, in the oldest age group, eight

respondents (62%) reported having weak computer skills. In addition, the charts below show that both confidence and skill level tend to decrease with age among the respondents. This finding is reflected in one participant's comment about internet affordability: *[It's] not always about affordability. Many seniors [are] not comfortable using computers.*
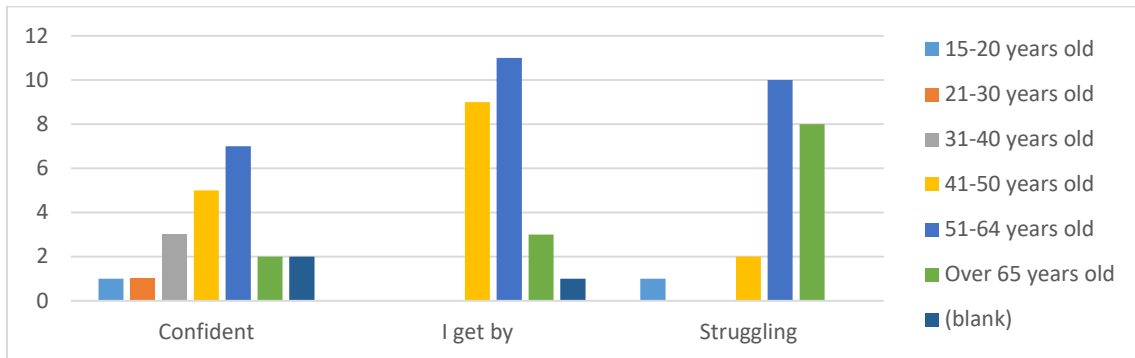
Confidence in digital skills by age (% calculated within each age group)

Age	Confident	Get by	Struggling	Total (n=63)
15-40	5 (83%)	0	1 (17%)	6
41-50	5 (31%)	9 (56%)	2 (13%)	16
51-64	7 (25%)	11 (39%)	10 (36%)	28
>65	2 (15%)	3 (23%)	8 (62%)	13

Computer skill level by age (% calculated within each age group)

| Age	Strong	Average	Weak	Total (n=63)
15-40	4 (67%)	1 (17%)	1 (17%)	6
41-50	7 (44%)	5 (31%)	4 (25%)	16
51-64	8 (28%)	10 (36%)	10 (36%)	28
>65	1 (7%)	4 (31%)	8 (62%)	13

When asked what kinds of computer skills they would like to learn more about, almost half of the respondents who answered this question (23) said they would like to learn "everything" about computers. Several others described specific skills they would like to learn, including keyboarding, creating and sending documents, using email and social media and surfing the

Internet. Others indicated an interest in learning more specialized skills such as using spreadsheets, how to set up a blog, web design, and coding or computer programming. A few also indicated that they would like to learn about how to protect their privacy online.

Computer skills you would like to learn	Responses (n=48)
General computer knowledge	23 (48%)
Office applications	9 (19%)
Programming	5 (10%)
How to protect privacy	6 (13%)
Social media	3 (6%)
None	2 (4%)

4l. Confidence using computers safely and knowledge of online privacy

Respondents were asked how they would describe their confidence level using the internet safely on a scale of one (weak) to five (strong). 20 people identified their confidence level as being very weak (1 on the scale) and 17 people said their confidence level was weak (2 on the scale). In other words, a total of 37 people, or 57% of respondents, felt that their confidence level regarding internet safety was weak. Eleven people (17%) indicated their confidence was average (3 on the scale), and 17 people (26%) reported strong confidence levels regarding safe internet practices.
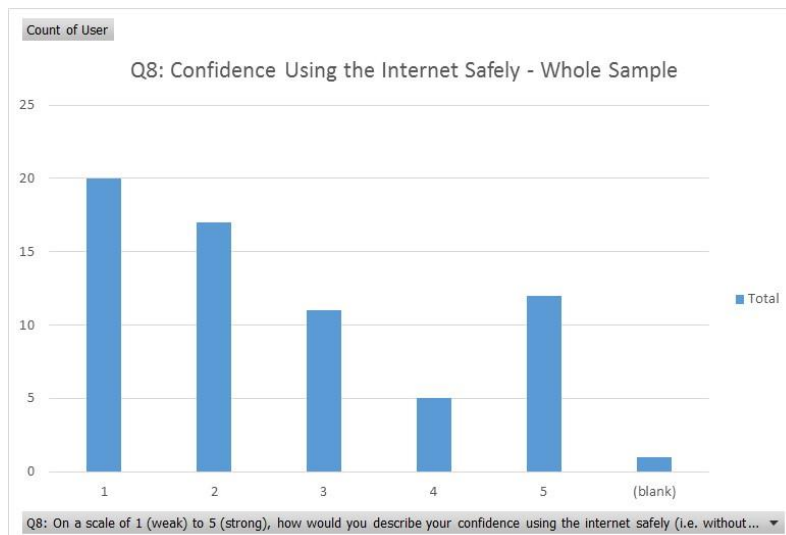
As shown by the charts below, when analyzed according to income level and age, findings show that respondents in the two lowest income categories report the lowest levels of confidence in using the internet safely (66% say their confidence levels are weak). Further to this, individuals in the higher age categories report significantly lower levels of confidence in using the internet safely than those who are under 41.

Confidence using the internet safely by income (% calculated within each income category)
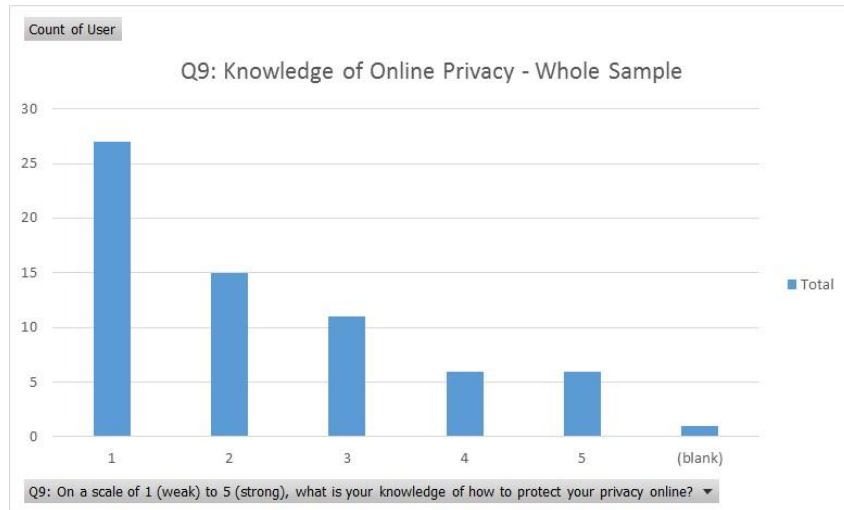
Income	Strong	Average	Weak	Total (n=53)
15-25,000	9 (22%)	5 (12%)	27 (66%)	41
More than 25,000	3 (25%)	4 (33%)	5 (42%)	12

Confidence using the internet safely by age (% calculated within each age group)

Age	Strong	Average	Weak	Total (n=57)
15-40	3 (60%)	1 (20%)	1 (20%)	5
41-50	4 (25%)	2 (12.5%)	10 (62.5%)	16
51-64	7 (29%)	2 (8%)	15 (63%)	24
>65	1 (8%)	2 (17%)	9 (75%)	12

When asked to rate their level of knowledge of how to protect their privacy online between 1 and 5 (1 being weak and 5 strong), 65% of respondents indicated 1 or 2. 11 people (17%) reported average knowledge of how to protect their online privacy, and 12 (18%) reported they felt they had above average knowledge.

Q9: Knowledge of Online Privacy - Whole Sample

Q9: On a scale of 1 (weak) to 5 (strong), what is your knowledge of how to protect your privacy online? ▼

These responses were also broken down according to income and age, showing that those with lower incomes were somewhat more likely to feel that their knowledge of how to protect their privacy online was weak. Age correlates to a more significant difference, however. 68% over the age of 41 described their knowledge of how to protect their privacy online as weak.

Knowledge of how to protect privacy online by income
(% calculated within each income category)

Income	Strong	Average	Weak	Total (n=53)
15-25,000	6 (15%)	7 (17%)	28 (68%)	41
More than 25,000	2 (17%)	3 (25%)	7 (58%)	12

Knowledge of how to protect your privacy online by age
(% calculated within each age group)

Age	Strong	Average	Weak	Total (n=62)
15-40	2 (33%)	2 (33%)	2 (33%)	6
41-50	2 (12.5%)	0	14 (87.5%)	16
51-64	6 (22%)	7 (23%)	14 (52%)	27
>65	1 (8%)	2 (15%)	10 (77%)	13

4m. What respondents would like to learn about online privacy

When asked to comment about what they would like to learn about online privacy, 17 respondents said "everything." Additionally, 20 people said they would like to learn about how to protect their privacy online, six said they would like to know how private the internet is, two wanted to learn about privacy settings, and one person said they would like to know which websites are trustworthy. Comments about what respondents would like to learn about internet privacy include:

> *How to protect myself while learning to use the computer* (B.C.)

> *How to avoid/be aware of fraud scams and to avoid virus downloads* (Nova Scotia)

> *What are the best ways to keep others out of my private info?* (Nova Scotia)

> *Privacy clauses – how to protect info when using it for online banking or shopping.* (Ottawa)

What would you like to learn about online privacy?	Total (n=47)
Everything about privacy online	17
How to protect privacy online	20
About privacy settings	2
How private Internet is	6
Which websites are trustworthy	1
Nothing	1

*4n. Concerns about online privacy*

When asked to comment on their concerns about online privacy, most comments focused on the general lack of privacy online (13) and how to protect it (9). Ten people were concerned about the security of their private information and identity theft. Protection of financial information was a concern for 7 respondents, and being spied on was a concern for 6 respondents. Two

people also identified concerns with scams and virus protection. Comments expressed concerns about a range of further issues:

That [lack of internet privacy] could primarily lead to a tyrannical society. (B.C.)

There does not seem to be a lot of privacy or a way to protect small kids from things they should not be exposed to. (B.C.)

There was a concern about personal liability as a resulting of a personal privacy breach: "That people take your information and do things with it and you can be held liable for it." Some people expressed a sense of insecurity dealing with personal information online. For example, one person said they "feel unsafe giving [information] of a private nature." Finally, several comments indicate that respondents were not sure what to be concerned about regarding online privacy. For example, one person said, "I have no views. Need to learn more about it," and another commented, "I was not concerned until I heard about this workshop."
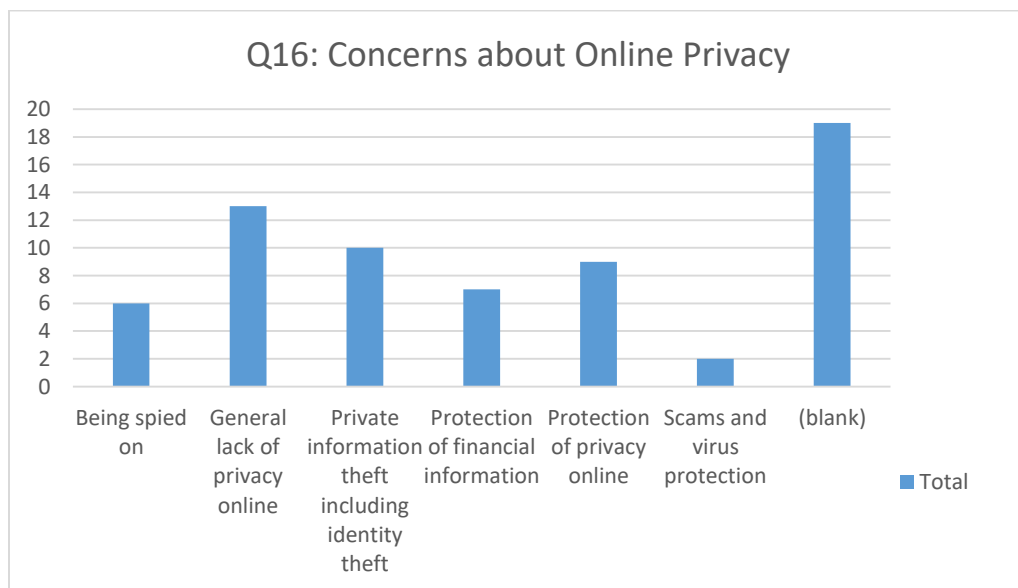
In all, the pre-workshop surveys suggest the powerful effects of income and age on Internet use and confidence to use the Internet. These are important dynamics to consider with respect to efforts to promote online privacy protection among and an engaged and vigilant citizenry. The following section presents findings of the post-workshop evaluations that point to the educational implications of these efforts.

Section 5. Findings of the Post-Workshop Evaluations

The post-workshop evaluations were intended to measure what participants learned in the workshops. We thematically summarize the responses to each question and include a few illustrative comments to add depth and texture to participants' answers.

5a. Summary of Reponses to Post-Workshop Evaluations

There was a total of 53 workshop evaluations completed across all regions. The number of completed evaluations is broken down by region in the chart below. In general, respondents indicated that they found the workshops to be very informative and that they learned a lot. The main areas of learning were

- increased knowledge of privacy rights through PIPEDA and the OPC and how to engage those rights
- awareness of the ways in which their privacy might be compromised in online environments
- strategies they can use to protect themselves on a regular basis

Responses throughout the evaluations suggest that more educational opportunities, perhaps with a variety of learning formats and with considerations around learners' language and literacy needs, would be welcome.

5b. Q1 – Overall, what was your opinion about the workshops?

Across the regions, 92% of participants found the workshops to be either "very informative" (31) or "informative" (18). One person thought the workshops were only "somewhat informative" and three felt they were "not very informative." Among those who responded "other," one person said there was "lots missing."

Overall opinion about the workshop by workshop location

City/Province	Very Informative	Informative	Somewhat Informative	Not Very Informative	Other	Total (n=53)
British Columbia	4	5	1			**10**
Nova Scotia	4	5				**9**
Ottawa, ON	9	3		1	2	**15**
Toronto, ON #1	8	1				**9**
Toronto, ON #2	6	4				**10**
Total	**31**	**18**	**1**	**1**	**2**	**53**

5c. Q2 – What topics or issues covered in this workshop are most important to you?

Participants found the workshops to be very informative overall. Specifically, respondents said they gained awareness of how their personal privacy may be compromised in online environments, by consumer tracking and biometrics. They also learned that they have rights to privacy, through PIPEDA and the OPC, and they learned ways to engage those rights such as by filing a complaint. People also said they learned about the need to take measures to protect themselves and found the practical suggestions offered by the workshop to be useful. Some of these strategies include safe banking practices, logging out of Facebook and other websites, turning off the GPS and locking their phones.

British Columbia

Respondents identified a variety of topics covered in the three workshops that were important to them. These include strategies to manage personal privacy and to consider what information one shares online, with the understanding that it is possible that this information can become public or viewed by unknown audiences for purposes over which they have little control. People expressed surprise over strategies that companies use to track online information and just how much of this information can be collected for unknown purposes. They appreciated strategies to limit the potential of companies to collect personal data and recognized that one must 'read the fine print.' One respondent found the amount of legal information about privacy issues hard to navigate, and another said they already knew most of the information.

Nova Scotia

Learning about issues around internet privacy was important to workshop participants. Participants were particularly interested in what their privacy rights are, safety practices while using the Internet, protecting personal information, and consumer information tracking. One person stated that through the workshop they became "aware of how much tracking was done with debit cards and store bonus point cards." Another participant learned always to log out of Facebook, and another mentioned that learning how to file a complaint was important. One person said they already knew the topics covered by the workshop.

Ottawa

The issue of personal privacy online and how to protect it also emerged as the issue of greatest importance to most people in this set of surveys. Participants were also concerned about the use of biometrics, internet tracking and the loss of control over one's personal information. One

person said they didn't learn anything new, and another said they would like to learn more about using computers.

Toronto – Workshop #1

From this workshop, most people reported that internet privacy and safety were important issues for them. This included learning about PIPEDA and OPC and their privacy rights as well as personal practices to increase internet safety. Participants mentioned changing passwords regularly, reporting breaches of privacy, how to protect personal information, protecting privacy while banking, and locking one's phone as important practical concerns that emerged from the workshop.

Toronto – Workshop #2

Several people said that all the issues covered by the workshop were important, while one person said, "most of it" was important. Participants also added that learning about privacy policies was important, as was learning about the language used to talk about internet privacy and ways to protect personal privacy (for example, reading terms and conditions carefully and the use of privacy settings).

5d. Q3 – What did you learn in this workshop that is new or surprising?

For participants, the workshops presented many new and surprising things. Most responses to this question indicate that the general area of privacy rights was new to them. They were surprised to learn about some of the ways that corporations and others can trace personal information. Information about through PIPEDA and the OPC, about what people's privacy rights include, and about the obligations of corporations was also new. Participants also learned that they have access to a complaint process if they feel their privacy has been breached and that

there is government support for this. In terms of individual measures to protect personal privacy, respondents learned that they can choose what information to disclose on line and other strategies to protect themselves. The fact that some respondents feel the digital "world is changing so much" signifies that there is a need for ongoing educational support.

British Columbia

Most people said the idea of 'privacy rights' was new to them. They were not previously aware that there are limits to how companies collect information and what they can do with it and that people have the right to complain when they feel their privacy has been breached. Exercising these rights seems more complex. People expressed surprise at the many ways that personal information is tracked, but that they can choose what information to disclose online. The idea that people have discretion over information they share (such as birthdates and so on) seemed new. Three respondents said they could not remember what was surprising or new for them. This suggests the need for ongoing workshops so that people can use these new ideas.

Nova Scotia

The information about PIPEDA, privacy rights and the obligations of corporations was new to some people. Others said that learning about how to protect themselves online was new. Two people said there was not much new in the workshop for them.

Ottawa

In general, participants were surprised by two things: the use of biometrics to track personal information and the use of GPS on phones to track people's activities. Three people said there was nothing new or surprising.

Toronto – Workshop #1

Participants learned that their personal information can be traceable on the internet without their knowledge, but that they have privacy rights through PIPEDA and OPC. They also learned that they can take measures to protect their personal information. For example, one person said they learned: "I was unsafe because I wasn't using good digital practices." Respondents mentioned that they learned "what to look for on websites and about what to do to report fraudulent activity," how to be sure a site is secure, and "who you can report spam to."

Toronto – Workshop #2

Two participants said there were a lot of new things in the workshop. One person said everything was new because "I was totally in the dark about computers" and another realized that "I need to learn more to make improvements," which indicates that more opportunities to become educated about internet privacy may be needed. Specific areas of learning included the terms that are used to talk about computers, particularly "cookies" and "metadata." Two respondents mentioned that they learned about getting information from government sources and two others indicated that they learned about protecting personal information. One person said that the world is changing so much that there was not much surprising in the workshop. This again suggests that as the digital world continues to evolve, so too will the educational needs of online participants.

5e. Q4 – Will you be able to use any of the information you learned in this workshop in your everyday life?

Almost every respondent answered "yes" to this question. Specifically, people said they would be more careful with their online practices and more cautious sharing personal information online. For example, some said they would be more careful to "read the fine print" and change

their privacy settings. The workshops raised awareness among participants about online security issues, about what they don't know and piqued their interest to learn more. Relatedly, it was identified that some may require help to apply what they learned. One participant raised the possibility of applying what they learned to helping others. These last two points suggest that for future collaborative learning opportunities may be appropriate.

British Columbia

Seven respondents said they would use the information they learned. For example, one stated, "I'm more aware about internet privacy and security, and making sure companies are reputable when ordering things online." Another expressed, "[This] peaked my interest more. I never thought about privacy before, this made me aware. It makes me think that we don't have any real privacy." Among those who said they would not use the information in their everyday lives, one was retired and we might infer did not use the Internet regularly, another did not remember the workshop content and the third gave no reason.

Nova Scotia

Seven people said they would be able to use the information they learned in the workshop in their everyday lives. Many participants said they would be more careful of their Internet practices. One person said they would more cautious to share personal information online, and another said they would change their privacy settings.

Ottawa

Thirteen people said the information learned in this workshop would be useful in their everyday lives. Three people specified by saying that they would take more precautions with online

activities. One person said, "it changed my way of thinking," and another said they learned how to find their phone if it gets lost. Two people said they didn't learn much they could use.

Toronto – Workshop #1

Everyone said they would be able to use the information from the workshop in their everyday life. One person said they already started doing so in the class. Another person said, "Yes, I will read the fine print, put locks on phone, change password often."

Toronto – Workshop #2

Everyone said they would likely be able to use the information they learned in this workshop in their everyday lives. One person said that they would need help doing so, and another person said they would use what they learned to help others. This suggests the need for ongoing educational opportunities but also that users can learn from and support one another.

5f. Q5 – Would you recommend this workshop to others?

Almost everyone responded "yes", they would recommend this workshop to others. The workshop was described as extremely beneficial. Since technology is always evolving, and "there are always new things to learn," participants would like to have similar educational opportunities in the future, possibly through ACORN. Seniors and newcomers to Canada were identified as groups who could benefit the most from further learning events.

British Columbia

All respondents said they would recommend this workshop series to others. One comment elaborated: "Most certainly I would encourage other people to take it, I would encourage ACORN to hold many more workshops like this and spread the word. There are so many people

that need this information, these workshops are very beneficial in this information age. This is a tool everyone should have." Another expressed that technology knowledge is evolving all the time and "there are always new things to learn." This again points to the need for ongoing educational opportunities.

Nova Scotia

All nine people in the Nova Scotia workshop said they would recommend this workshop to others. One person elaborated by saying the workshop was "well-presented and informative" and another said, "I am more mindful of the context in which I say certain things online."

Ottawa

Thirteen people said they would recommend this workshop to others. One said they would not. Another person said the "workshop should be more prepared."

Toronto – Workshop #1

Everyone said they would recommend this workshop to others. Two people said the workshop would be especially useful to newcomers and seniors, and two others said, "everyone should know." The point about newcomers and seniors is consistent with findings that suggest older adults are less confident in their digital skills and require support and that language and literacy needs also need to be addressed in digital learning.

Toronto – Workshop #2

Everyone said they would recommend the workshop to others. One person said, "Yes, it is informative" and another pointed out that it would be especially useful for older people, again reinforcing the suggestion that older adults have unique digital literacy needs.

5g. Q6 – What suggestions would you give to improve this workshop?

The suggestions that came out of this section centre around issues of language and literacy, content delivery format, and the need for ongoing educational opportunities. As noted above, aspects of the responses suggest that some respondents may not be native speakers of English and some may have literacy challenges. This background informed our understanding of participants' suggestions for improving the workshop. People suggested that the language of delivery should be simple and easy to understand. It was suggested that print materials also be provided and that both print and electronic text be in simple clear language with large font size and simple colour contrasts for visibility.

Participants were interested in having a diversity of learning formats. In addition to the presentation style of learning, they indicated an interest in hands-on learning with devices. Collaborative learning was also suggested as another format, as well as having direct personal help from facilitators. It seems that in one of the workshops respondents felt that their participation was not treated equitably, so providing a more diverse approach to learning may help to resolve this kind of situation.

In addition, participants expressed the need for more learning opportunities about this topic. It was suggested that the workshop could have been longer and that more similar workshops should be offered. Finally, it was pointed out that food should be offered since one of the workshops happened at meal time. Perhaps the nutritional needs of participants can be taken into consideration.

British Columbia

Four respondents said they would change nothing about the workshops. Other suggestions included offering handouts, making it easier to understand, having devices on hand to practice,

making the workshop longer, and providing more workshops, as "there is so much that needs to be explored." These suggestions were consistent across the regional workshops.

Nova Scotia

Five respondents said they were satisfied with the workshop and did not have suggestions for improvement. One person said it was "very well put together" and another said, "it was very informative and covered a lot." One person suggested the workshop should include more group activities. One person said, "I was expecting more from the workshop. It was everyday common sense stuff I already knew. Maybe it would be useful for some people, but for me it wasn't helpful." This comment suggests that it may be helpful for potential participants to be informed about the workshop content before they participate.

Ottawa

A few people were interested in having some hands-on learning with devices (computers and phones) so they could learn about how to apply the new information in a practical way. One person suggested that the workshop offer more details on how law enforcement monitors activity, and another suggested that they would have like to know the source of the information provided. From a workshop facilitation perspective, two respondents said that the facilitator should have managed the discussion better, as some attendees seemed to be dominating. Another requested that the facilitator use white instead of brown charts and increase the font size. One person said that because of the time of the day, it would have been nice to have some food. Another respondent suggested that the intake questionnaire could have turned the "'discomfort with others knowing info about you' into a box-ticking questionnaire to gather data on how unaware or competent respondents are."

Toronto – Workshop #1

Most people said there is nothing to add to improve the workshop. However, one person said it would be helpful if the vocabulary were simpler so everyone could understand.

Toronto – Workshop #2

Several people suggested that the workshop be longer and that more similar workshops be offered. One person suggested that the workshop could offer more details and that facilitators "can help you," again suggesting that direct personal support would be a helpful addition to the workshop. Another said the workshop "can be done better for improvement" but did not offer specific suggestions. One person said they had no suggestions for improvement.

Section 6. Summary of findings, conclusions and recommendations

A clear need for ongoing privacy education. There is clearly strong interest and need for community-based education about Canada's privacy legislation, the responsibility of agencies and businesses that conduct business online, the risks to personal privacy of some online activities, and strategies that everyday citizens can deploy to protect their information and their privacy. Respondents found the workshops very informative and would recommend them to others. Responses to the pre- and post-workshop surveys also suggest that people found information about the prevalence of online tracking, monitoring, and data mining to be new and interesting. This suggests that people are largely unaware of these activities and indeed may feel powerless to control them without access to these workshops. As we have noted, the Internet and its many technologies are constantly evolving, and timely and ongoing education is necessary so

that all citizens have equal access to the information and skills they need to safely use the Internet.

Digital equity, education and the protection of online privacy are interconnected. The survey results, supported by literature presented in Section B, suggest that the responsibility for protecting online privacy is shared among Internet users, businesses and by government policy and legislation. Here, equity in access to the Internet is vital; the surveys show that 17% of respondents rely upon public computing spaces to access the Internet. Therefore, it may be prudent to consider the Internet security issues that may exist for this group and possible strategies they need to know to protect themselves.

Another significant group of respondents reported making sacrifices in other areas of basic need to afford home Internet. These users are vulnerable to changes in Internet pricing, which may push them offline or into reliance upon public computers. The nature of devices people use to access the Internet is also important to the privacy issues they might encounter: those who rely on public access computers or unsecured Wi-Fi in lieu of cell data may be more vulnerable to security breaches and personal data theft than those who have access to secure servers, an issue that would benefit from further research. Income was correlated with reported skill and confidence using the Internet. Income might be interpreted as a dynamic of use and time online, as well as age. In other words, income is tied in with other factors that impede computer confidence, a phenomenon that can be addressed by making the Internet more affordable and through ongoing access to digital education. As we move into a more fully digital culture and economy, the entanglement of privacy protection with digital equity will benefit from further research and further initiatives such as ACORN Canada's *Protect your Privacy-Online!*

Online privacy education: Implications for design and delivery. The survey results suggest several implications for the design and delivery of digital literacy education oriented to protecting privacy online:

1) Print materials and oral language used in workshop delivery need to be considered with the audience in mind. Materials should be clearly laid out, use principles of clear language (cf. Clear Language and Design, 2015) and include illustrations as much as possible.

2) Experiential learning activities: People appreciate opportunities to try new skills during the workshop; time for hands-on learning, preferably with people's own devices, will increase the chances that the skills they learn are transferable to other contexts;

3) Workshop facilitation should include one-to-one support. Including additional instructors or peer tutors may support this. People might be reticent to ask questions in a group setting, or to share information in a large group. In workshops about privacy, there should be opportunities for private conversations and one to one support in addition to small and whole group learning;

4) Workshops should be offered on an ongoing basis so that people can refresh their skills and learn new information over time, rather than as a 'one-off' event. Indeed, the most successful forms of education are those that allow people to build on their knowledge over time, ask questions and receive one-to-one support.

In conclusion, *Protect Your Privacy-Online!* is a unique pioneering initiative that has supported the digital education of low income citizens in this vital and often neglected area of digital education. The workshops were very well received by communities, and the project has opened

new sources of information and insight about the relationship between digital equity and the

protection of privacy online. Indeed, low income and older citizens seem particularly vulnerable

to breaches and threats to online privacy. Ongoing workshops and education such as *Protect

Your Privacy-Online!* that are accessible to communities seem particularly important, as is

continuing research into the relationships between online privacy protection, education and

digital equity.

Works cited

ACORN Canada (January, 2016). *Internet for all: Internet use and accessibility for low income* Canadians. Author: Ottawa, ON.

Best, K. (2010). Living in the control society: Surveillance, users and digital screen technologies. *International Journal of Cultural Studies, 13*(1), 5-24. doi:10.1177/1367877909348536

Burns, T. and Novacs, R. (October 9, 2014). Infinite connections: The digital divide. Education today. Retrieved from http://oecdeducationtoday.blogspot.ca/2014/10/infinite-connections-digital-divide.html

Canadian Broadcasting Corporation (CBC) (April 6, 2012). *Ottawa cuts CAP public web access funding*. Retrieved from: http://www.cbc.ca/news/canada/nova-scotia/ottawa-cuts-cap-public-web-access-funding1.1152248

Canadian Centre for Policy Alternatives (CCPA) (2012). *The Internet tree: The state of telecom policy in Canada, 3.0.* Ottawa: Author.

Clear language and design (CLAD). (2015). *Tips and tools for clear language and design*. Retrieved from: http://clad.tccld.org/category/tips-tools/

Gilbert, M. (2010). Theorizing digital and urban inequalities. *Information, Communication & Society, 13*(7), 1000-1018. doi:10.1080/1369118X.2010.499954

Haight, M., Quan-Haase, A., & Corbett, B. A. (2014). Revisiting the digital divide in Canada: The impact of demographic factors on access to the internet, level of online activity, and social networking site usage. *Information, Communication & Society, 17*(4), 503-519. doi:10.1080/1369118X.2014.891633

Industry Canada (2015a). Digital Canada 150: Retrieved from http://www.ic.gc.ca/eic/site/028.nsf/eng/home

Mossberger, K., Tolbert, C., & Franko, W. (2013). *Digital cities: The internet and the geography of opportunity.* New York: Oxford University Press.

OECD (2015). Infinite connections: Education and new technologies. *Trends shaping education Spotlight 5:* Retrieved from: http://www.oecd.org/edu/ceri/Spotlight%205-%20Infinite%20Connections.pdf

Public Interest Advocacy Centre (March, 2015). *No Consumer Left Behind: A Canadian Affordability Framework for Communications Services in a Digital Age.* Retrieved from http://www.piac.ca/wp-content/uploads/2015/03/PIAC-No-Consumer-Left-Behind-Final-Report-English.pdf

Sloan, R. H., Warner, R., & EBSCOhost. (2013). *Unauthorized access: The crisis in online privacy and security.* Boca Raton, FL: CRC Press.

Statistics Canada (2013). *The daily: Individual internet use and e-commerce.* Retrieved from: http://www.statcan.gc.ca/daily-quotidien/131028/dq131028a-eng.htm.

About the authors

[i] Sherry Breshears is a doctoral candidate in Education and Labour Studies at Simon Fraser University.

[ii] Suzanne Smythe, PhD, is Assistant Professor in Adult Literacy and Adult Education in the Faculty of Education, Simon Fraser University.

APPENDICES

APPENDIX A – Workshop 1 "PIPEDA and You: Know Your Privacy Rights and Protect Your Info Online!" Lesson Plan

APPENDIX B – Workshop 2 "Digital Trails: Managing your Online Profile & Our Bodies as Information: Wearable Computing and Bodily Tracking Devices" Lesson Plan

APPENDIX C – Workshop 3 "Personal Information as a Commodity: How the Private Sector uses Your Online Personal Information & Who is watching you? Government Services and Surveillance Online" Lesson Plan

APPENDIX D – Pre-Workshop Questionnaire

APPENDIX E – Post-Workshop Evaluation