International Journal of Communication 11(2017), 2784–2805 1932–8036/20170005

Open Privacy Badges for Digital Policy Literacy

KAREN LOUISE SMITH[1]
Brock University, Canada

LESLIE REGAN SHADE
University of Toronto, Canada

TAMARA SHEPHERD
University of Calgary, Canada

Previous work on digital policy literacy in relation to youth and privacy highlights that youth need to comprehend policy processes, the political economy of media systems, and sociotechnical infrastructures. Understanding in these domains is necessary for youth to negotiate both their social and informational privacy and to engage with the terms of service of the platforms they regularly use. In this article, we examine the digital policy literacy implications of a codesign project with eight teenagers whose goals were to create prototype-level open badges relevant to digital privacy in the Canadian context. We argue that codesign, informed by the culture of open source software, empowerment approaches to privacy education, and connected learning can provide new avenues to enhance digital policy literacy among youth.

Keywords: privacy, youth, codesign, participatory design, social media, open source

Introducing the Privacy Badges Project

Picture a Saturday morning in October, in Toronto, Canada. Just south of the Queen West neighborhood, a design research team is assembling for the first time in a low-rise office building that is home to Mozilla. The design research team comprises eight teen peer researchers, academics, and Mozilla staff. Mozilla is a global nonprofit organization, well known for its open source Firefox Web browser. The

Karen Louise Smith: karen.louise.smith@brocku.ca
Leslie Regan Shade: leslie.shade@utoronto.ca
Tamara Shepherd: tamara.shepherd@ucalgary.ca
Date submitted: 2016–08–09

[1] We thank the teen peer researchers and Mozilla staff, in particular Kathryn Meisner and Doug Belshaw, who were critical to the project's execution. This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the authors and do not necessarily reflect those of the OPC.

design research team is not tinkering with Firefox, however. The members are clustered around a whiteboard featuring 10 empty hexagon-shaped figures. The hexagons are the opening template for a six-month challenge for the design research team. Their collective task is to codesign 10 prototype-level open privacy badges and associated teaching activities in the form of open educational resources (OERs).

As described by Atkins, Brown, and Hammond (2007), OERs "are teaching, learning, and research resources that reside in the public domain or have been released under an intellectual property license that permits their free use or re-purposing by others" (p. 4). OERs build on the culture of open source software, which is distinguished from proprietary software because it enables users to access, alter, and redistribute the source code of the programs they use. Although Mozilla is best known for developing open source software, it also creates OERs to support Web literacy in diverse communities globally. Mozilla describes Web literacy as the ability to read, write, and participate on the Web (Belshaw, Smith, & the Mozilla Community, 2014; Mozilla, n.d.), which overlaps significantly with various definitions of digital literacy. Broadly speaking, *digital literacy* refers to the technical, cognitive, and sociological skills needed to perform tasks and solve problems in digital technology environments (Eshet-Alkalai, 2004; Meyers, Erickson, & Small, 2013; Tyner, 1998). Fluency in digital practices is seen as significant not only as the basis for a thriving digital economy but also for a more connected and engaged citizenry (Jenkins, Ito, & boyd, 2015; Kellner, 2002; Meyers et al., 2013).

Many organizations, ranging from the World Economic Forum to Mozilla, are interested in assisting people to transition from passive consumers to creators of the Web (Mozilla, 2015; World Economic Forum, 2012). In Toronto, Web literacy initiatives and OER creation are championed locally by the Mozilla-stewarded Hive Toronto Learning Network. The network includes more than 60 organizational members, primarily from the informal learning sector, including public library systems and after-school programs. Hive Toronto, open badges, as well as other OER infrastructures in use at Mozilla provided a base for the privacy badges project to build on.

Open badges and Hive Learning Networks have received support from the MacArthur Foundation (Mozilla Hive New York, n.d.; Mozilla Open Badges, n.d.). Partnering with the MacArthur Foundation, Mozilla's emphasis on the participatory creator in its digital literacy initiatives pushes a "more radical understanding" within the field, as Meyers and colleagues (2013) contend. Various initiatives at Mozilla, derived from the open source culture and infrastructural aspects of the Web for education and learning, nurture this flavor of creative digital literacy as "maker" or "hacker" literacy. Sandvig (2013) similarly identifies that the Web is an infrastructure "which is foundational to other activities" (p. 86), and Mozilla adheres to this logic by attempting to build greater openness in education on the successes of its open source software community. For example, Mozilla provides openly licensed teaching activities, which it encourages the community to adapt, as well as open source software tools (https://learning.mozilla.org/tools) to teach coding and remix (Santo, Ching, Peppler, & Hoadley, 2016; Smith & Belshaw, 2015). Open badges are another such infrastructure that Mozilla supports. Grant (2014) describes an open badge as an "image file embedded with information" (p. 7) that can be used to recognize learning or an accomplishment. Open badges rely on an open technical standard so that anyone can issue badges online. The privacy badges project thus aimed to leverage Mozilla's Web literacy and

educational infrastructures to encourage youth to create for the Web as they also learned about digital privacy.

Some contextual and social dimensions of infrastructure (Bowker, 1994; Star, 1999) are also relevant to the privacy badges project. As innovative models in the learning sector, both the Hive Learning Network model and open badges received support from the MacArthur Foundation in the United States to become established as sociotechnical infrastructures and examples of connected learning (Grant, 2014; MacArthur Foundation, 2010; Mozilla Hive New York, n.d.; Mozilla Open Badges, n.d.; Rafalow & Larson, 2014). Connected learning "advocates for broadened access to learning that is socially embedded, interest-driven, and oriented toward educational, economic, or political opportunity" (Ito et al., 2013, p. 4). Building on its work to "tap . . . the opportunities provided by digital media" and address "equity gaps" (Ito et al., 2013, p. 4), the Hive Toronto privacy badges project used existing connected learning models and infrastructures in the creation of open badges to bolster openness and also enhance opportunities in the informal learning sector. Open badges were selected as a key technology for this project because of their potential as "a viable alternative to existing methods of assessment" (Halavais, 2011, pp. 354–355), in which attempts can be made to create symbols of recognition for what a community values. In addition to sharing some of the aspirations for badges, Halavais cautions that "badges have baggage" and their history includes "a more regimented and hierarchical past" (pp. 354–355).

With awareness of both the strengths and weaknesses of badges, the design research team created an ecosystem of 10 open privacy badges at a prototype level. The badges were suitable to engage teens to learn about privacy in informal learning settings (e.g., public libraries and community centers) and in civic learning contexts. The teen peer researchers in the project each contributed an average of 53.9 project hours over the six-month duration of the project. In this article, we describe how the codesign project supported the development of digital policy literacy with youth through an exploration of policy processes and engagement with the political economy and sociotechnical infrastructures of the Web.

Theoretical and Methodological Approach for a Privacy Codesign Project

The privacy badges research and codesign project at Mozilla was made possible by funding from the Office of the Privacy Commissioner of Canada during the first author's (K.L.S.) engagement with Mozilla and Hive Toronto as a postdoctoral fellow via the Mitacs Elevate program in Canada. The Office of the Privacy Commissioner of Canada's Contributions Program supports research and education projects that relate to personal information in the corporate sector, consistent with the Personal Information Protection and Electronic Documents Act (PIPEDA) privacy legislation in Canada. PIPEDA first came into effect in 2000, and it pertains to how personal information can be collected, used, and disclosed in the private sector.

In addition to PIPEDA, the privacy badges project was informed by an array of theoretical and methodological approaches concerning privacy, digital policy literacy, and codesign. Beginning with key definitions of privacy as contextual integrity and networked privacy, this section reviews the literature from these areas that is relevant for understanding the privacy badges project as an initiative oriented toward an empowerment approach.

Approaches to Understanding Privacy

When exploring the concept of privacy in a networked environment, it is perhaps most expedient to begin with the euphemism "It's complicated," popularized by Facebook for relationship status updates. With regard to privacy education, Steeves (2010) identifies how "educational initiatives that focus on teaching children not to disclose personal information because of safety risks are limited because they are out of step with what children know about and experience on the Internet" (p. 4). Steeves emphasizes that youth use digital media for formative everyday activities including exploring identity, building connectedness, and validating the self. Given the diversity of such activities, a set of complementary approaches for understanding privacy—including privacy as contextual integrity, networked privacy, and empowerment approaches to privacy—were drawn on to frame the privacy badges project.

Nissenbaum's (2011) concept of privacy as contextual integrity begins from the assumption that people's lives unfold in a variety of settings, including diverse face-to-face and computer-mediated interactions (see also Nissenbaum, 2004). Nissenbaum argues that privacy must involve adherence to the appropriate information-sharing norms for each and every social context, which are often overlapping and nondiscrete. Nissenbaum (2004) also identifies that privacy debates are often constrained by the conception of the Web as merely a commercial space, whereas for many people, their multiple uses of the Web beyond commerce accord it the status of a necessary public good.

Since the widespread popularization of Web-based communication, various scholars have also considered the modulations to privacy in a socially networked age (e.g., Agre & Rotenberg, 1998; boyd, 2012; Raynes-Goldie, 2010). For networked privacy to be explored, boyd (2012) suggests that scholars "develop models that position networks, groups, and communities at the center of our discussion" (p. 350). Instead of denigrating youth for using social media and the Web more broadly, boyd encourages a reconsideration of the concept of privacy for the networked lives of youth. This perspective has informed more recent literature on youth and online privacy, which tends to acknowledge young people's agency in negotiating privacy in different kinds of online spaces (e.g., Marwick & boyd, 2014; Vickery, 2015).

Contemporary debates concerning youth and privacy thus argue for moving beyond framing youth simply as surveillance subjects. Consistent with the ideas of contextual integrity and networked privacy, Regan and Steeves (2010) argue that the peer-to-peer interactions characteristic of social media and the Internet more broadly can facilitate the opportunity for youth to empower themselves in relation to privacy issues. They suggest that empowerment when under surveillance requires attention to settings where there is "two-way" surveillance, which encourages youth to understand the working of surveillance and perhaps even hold their watchers accountable.

Together with boyd's idea that groups and communities should be considered in relation to privacy and Nissenbaum's (2011) acknowledgment of noncommercial online spaces, Regan and Steeves's (2010) work on empowerment approaches to privacy provides intellectual scaffolding for the privacy badges project. Regan and Steeves draw on Amichai-Hamburger, McKenna, and Tal (2008) to suggest four levels of empowerment that can be considered in relation to youth privacy: (1) individual, where people may gain new digital skills; (2) interpersonal, where they may create and sustain relationships; (3)

group, where challenges may be faced collectively to stem isolation; and (4) citizenship, where youth can work with others to challenge the status quo. In this way, empowerment approaches to privacy not only implicate the agency of youth to negotiate their own privacy expectations but also to contribute to policy formation around online privacy and surveillance (e.g., Montgomery, 2015). Empowerment at each of the levels proposed by Regan and Steeves was present in the privacy badges project and can be mapped onto the digital policy literacy framework.

Digital Policy Literacy Framework

A key goal of the digital policy literacy framework has been to expand the realm of media literacy to encompass digital policy. Earlier work has applied the digital policy literacy framework to consider youths' knowledge of mobile privacy and their perception of telecom provider constraints (Shade & Shepherd, 2013) and an assessment of youths' negotiations of usage-based billing and consumer activism (Shade, 2015). Three elements compose the framework of digital policy literacy.

Policy processes. This element seeks to understand policy processes and asks how policy is constituted. What are structures of participation in policymaking? What are effective modes of activism and intervention to shape policy?

Political economy of media systems. This element seeks to understand the social, political, and economic factors associated with communication and media systems, and asks, what are the sociopolitical relations surrounding the ownership, production, distribution, and consumption of media? And, how do these structures reinforce, challenge, or influence social relations of class, gender, and race?

Infrastructures. Infrastructures are sociotechnical systems in that they combine the material technologies for digital connectivity with the human relationships implicated in their design and use (see Bowker, 1994; Star, 1999). This element seeks to understand how technological affordances and design activate or inhibit online interactions, and asks, what is the impact of affordances and design on ownership of content, privacy protection, access, and communication?

Codesign Methods

Participatory Design, or Codesigning With Youth

Having briefly reviewed the relevant literature on privacy and the digital policy literacy framework, the codesign workshops held with youth peer researchers require some explanation. The project began by considering privacy as a contextually situated experience by youth, which frequently involves networked environments. The codesign methods of the privacy badges project were influenced most directly by the participatory design tradition, which originated in Scandinavia in the 1970s. Participatory design is achieved when "the people destined to use the system play a critical role in designing it" (Schuler & Nakioma, 1993, p. xi). *Codesign* is a related term, which is sometimes used at Mozilla to describe interactions between learners, educators, and the organization as Web literacy projects are developed (e.g., Mozilla Clubs, n.d.). This is consistent with the scholarly literature, including the work

of Sanders and Stappers (2008), who use the term *codesign* "to refer to the creativity of designers and people not trained in design working together in the design and development process" (p. 6).

Some privacy-relevant design research projects with youth engage in such codesign and participatory methods. For example, Raynes-Goldie and Allen (2014) involved youth as coparticipants in the research and design of a video and board game hybrid called "The Watchers." Muller, Timmermann, Fortmann, Heuten, and Boll (2013) collaborated with girls to create an app for privacy-aware location sharing. Similarly, the teen peer researchers who were engaged in the privacy badges project became design collaborators to create prototype-level badges as well as OERs.

As a part of the project, workshops were held on seven dates (typically Saturdays) between October 2014 and February 2015. All protocols for the project underwent ethical review at the University of Toronto, consistent with the Tri-Council policies, which govern research with human participants at Canadian universities.[2] The teen peer researchers consisted of eight high school students and one postsecondary student, ages 15–19, with diverse genders and cultural backgrounds. Half of the peer researchers were previous volunteers or participants at Hive Toronto organizations related to digital literacy and coding. They were recruited through site visits to Hive Toronto organizations, posters, and the project website, and their contributions to the project were recognized through the honorarium of gift cards, at a value of $12.50 per hour of project engagement. Parents or guardians were involved in the project consent and assent process for all youth under 18 years of age. As an ethical safeguard, participants were also free to quit the project at any point and to opt out of any project components.

During workshops, teen peer researchers participated in activities such as brainstorming, ideation, prototyping, documentation, and trialing prospective badge activities. Peer researchers also conducted interviews with one another and presented their thoughts and projects to the group. In between workshops, teen peer researchers could complete homework activities (i.e., watch YouTube videos relevant to privacy, or sketch a new badge concept) and share their results through a threaded discussion board and team collaboration site called Minigroup, which is now a defunct service.

The privacy badges workshop format built on ideas including boyd's (2012) suggestion that groups be central to privacy inquiry, as well as those constitutive of connected learning scholarship (e.g., Ito et al., 2013). Ito et al. (2013) describe that connected learning is achieved when "a young person is able to pursue a personal interest or passion with the support of friends and caring adults, and is in turn able to link this learning and interest to academic achievement, career success or civic engagement" (p. 42). In the case of the privacy badge participants, youth completed an average of 53.9 hours of project engagement and were eager to leverage their experience toward their postsecondary educational and extracurricular goals. Participants in the privacy badges workshop also showed some interest related to civic engagement and privacy, as explained in the Results and Discussion section.

[2] Coauthors Smith and Shade were situated at the University of Toronto during the project.

Interviewing and Knowledge Mobilization With Educators

Educators' insights were also incorporated into the privacy badges project. During the course of the project, two adult team members interviewed 16 informal educators (e.g., youth workers, librarians, and others working outside the school system) for feedback on the badge system. To further incorporate educators' perspectives and develop awareness of the OERs, the design research team held a knowledge mobilization event in February 2015 for 37 educators and members of the public. This event created an opportunity for the peer researchers to introduce the badges to community organizations that would be likely to use them in their youth programming.

Results and Discussion

The array of research methods used for the privacy badges project produced a variety of results. The codesign methods led toward the creation of OERs including badge prototypes and teaching activities. During the codesign process, the teen peer researchers also provided insights that are relevant to empowerment approaches to privacy, and contribute to building a more robust understanding of what the digital policy literacy framework means in the context of a research project that is informed by participatory means of creating both technologies and knowledge.

The Privacy Badges OERs

The privacy badges project resulted in the successful codesign of OERs consisting of the 10 privacy badges and associated learning activities. The 10 privacy badges can be arranged under four overarching themes: personal information, privacy in everyday life, privacy policy, and privacy futures (Smith, Meisner, Shade, Shepherd, & Belshaw, 2015; see Table 1). The themes are overlapping, with some badges cross-listed between themes. With the curriculum made available online, organizations are encouraged to take up any combination of the badges and to remix the resources to suit their purposes (http://hivetoronto.org/portfolio/privacybadges/).

Three of the badges (Data Trail Timeline, IP Tracer, and Privacy Coach) were digitally earnable on a Mozilla site in Spring and Summer 2015. As a core outcome of the project, Mozilla has since implemented these three learning activities in its global Protect Your Data privacy teaching activities, which are available online (https://learning.mozilla.org/activities/protect-your-data/). In addition, Mozilla featured the IP Tracer as a summer learning activity in 2015 for its global community (Mozilla, 2015).

Table 1. The 10 Prototype-Level Open Privacy Badges.

Personal information	Privacy in everyday life	Privacy policy	Privacy futures
Anonymizer	Data Trail Timeline[a]	Requester[a]	Internet of Things
IP Tracer	Mobile	Profiler	Drones[a]
	Privacy Coach[a]	PIPEDA Remixer	

Note. PIPEDA = Personal Information Protection and Electronic Documents Act.
[a]Badge is cross-listed between themes.

IP Tracer *Profiler* *PIPEDA Remixer*

Figure 1. Three open privacy badges.

Three of the badges from the project, IP Tracer, Profiler, and PIPEDA Remixer (see Figure 1), are discussed in relation to youth empowerment and the digital policy literacy implications of this codesign project.[3]

Empowerment Through Codesign

The empowerment approach to youth privacy discussed by Regan and Steeves (2010) suggest that youth interest in privacy may be triggered by their usage of the very platforms that facilitate their surveillance. This line of thinking was directly articulated by youth participants in interviews and activities associated with their motivations for being involved in the codesign project. Participants demonstrated an awareness of the commercial status of social media platforms; for example, one participant stated, "It's very interesting to see how teenagers are impacted by privacy in their daily lives because obviously we use a lot of social media like Facebook [and] Twitter" (Teen 1, peer interview).[4] The teen also stated, "I think my main interest is seeing how exposed we are every day in terms of what kind of data we're leaving behind, what kind of data businesses are collecting every day" (Teen 1, peer interview). Teen participants in the codesign workshops similarly expressed some concerns about whether their online data is protected: "We're constantly seeing cases in the news with people who don't know about their rights, their privacy is breached, and they really don't know what's going on" (Teen 7, peer interview).

---

[3] The privacy badge iconography was designed using Font Awesome by Dave Gandy (http://fontawesome.io), and its open licensing allows for reuse in open source and also commercial projects. All badges from the project are available under a Creative Commons Attribution 4.0 International License. Thank you to Ashley Jane Lewis for badge design work.

[4] In this article, participant numbers and not gender pronouns identify the teen peer researchers. The peer researchers are thanked by their first names on the project home page, and their participation in the project is not fully anonymous as per consent and assent processes. Adult interview participants are described by their professional roles.

Through the workshops with youth, a variety of practices and activities were discussed by the teens that relate to the individual, interpersonal, group, and citizenship levels of empowerment formulated by Regan and Steeves (2010) in relation to privacy. Although the workshop activities did not directly require youth to change any of their practices related to personal accounts, they described numerous instances in which they made changes at the individual and interpersonal level. The group dynamic of the codesign workshop and citizenship implications were also discussed.

At the individual level, participants in the workshop noted changes that related to their participation and engagement with online environments outside the workshops. For example, one participant spoke of "using in-private browsing more" (Teen 4, staff-led interview). Another teen noted that they updated their passwords after their participation in codesign workshops: "Two weeks ago I changed all my passwords. I used to have the same two passwords that I would alternate for all my accounts, and I just realized that that's not safe at all!" (Teen 2, staff-led interview).

At the interpersonal level, peer researchers also reflected on changes around how they maintain and sustain relationships online. One teen described, "After the first workshop, I changed the privacy settings on my Facebook" (Teen 8, staff-led interview). Another peer researcher told us how they altered their Facebook interactions to be more customized for different friend groups: "I went through my Facebook and put special settings for people that aren't close friends, just people I kind of just know" (Teen 5, staff-led interview).

The group environment of the codesign workshops also scaffolded toward empowerment for the teen peer researchers. One peer researcher shared thoughts on the group dynamic to explore privacy:

> Being part of this peer research project is unlike anything I have done before, and I did not know what to expect. However, the project was explained to us well, we went over our hopes and fears, and we set guidelines for what we expected of ourselves. The first workshop helped put aside fears like not knowing enough about privacy or technology, so that was very reassuring. (Teen 1)

Similarly, another teen commented,

> I find it really enriching because it opens my mind into all these different things I never even thought about. . . . I've really enjoyed all the diversity we've had in the workshop and being able to discuss ideas with other people who are my age. (Teen 4, staff-led interview)

One of the project participants (Teen 3) noted that they interacted with the privacy badge peers differently than youth they encountered in other settings. Where the teens' normal practice would be to add others as friends on Facebook, that interaction seemed inappropriate to them in the context of the privacy badges group.

At the citizenship level, the workshops were also influential for youth peer researchers. Over the course of the workshops, teen peer researchers commented on their growing awareness of privacy issues, which included an increased awareness of PIPEDA and privacy law:

> Before I started this research project I honestly knew nothing about PIPEDA and how much of my information is collected and saved. It scares me now to think how oblivious youth is to prying eyes of the Web. The biggest privacy issue facing teens is [definitely] that of lack of knowledge. (Teen 8, Minigroup post)

In addressing this lack of knowledge about privacy law, the project also pushed teen peer researchers to connect legislative issues with their everyday experiences of digital culture, as elaborated below. Organizing these findings according to the digital policy literacy framework illustrates how policy processes, political economy, and infrastructures intersect as complementary dimensions of online privacy awareness. Furthermore, the digital policy literacy model enables us to draw out the significance of an empowerment approach to privacy as it played out in the codesign of specific badges.

Policy Processes

As described in the previous section by Teen 8, learning about PIPEDA was an element of the privacy badges project. As outlined in the digital policy literacy section, policy processes that are relevant to privacy involve an array of actors including governments, corporations, and citizens who make decisions relevant to privacy.

In the Canadian context, PIPEDA governs personal information that is collected for commercial purposes. Under PIPEDA, the term *personal information* refers to data about an identifiable individual. An Internet protocol (IP) address is deemed to constitute personal information in Canada or personal data in the European Union; however, its collection and use are less protected in the United States (European Parliament, 2013; Office of the Privacy Commissioner of Canada, 2013; Rich, 2016).

From the privacy badges curriculum, the IP Tracer badge was pivotal to illuminate certain aspects relevant to the politics of IP address collection, as well as geolocation (see Figure 2). In brief, an IP address is a string of numbers, such as 139.57.153.157, that typically acts to identify a device in a network. During the IP Tracer learning activity, participants were tasked to find the IP address of a laptop or other device. Participants also looked up the IP addresses of websites they visit on a regular basis, such as Wikipedia.org, or Instagram.com. The IP Tracer activity revealed for participants that there are geographic aspects to the Internet and that they (or their data) can be geolocated.

Figure 2. The IP Tracer badge.

Over the course of the privacy badges workshops, youth had a variety of reactions to the IP Tracer badge and geolocation more broadly. Teen 8 noted that they found it helpful to "engage in hands-on activities like actually tracking an IP [address] . . . instead of reading excerpts and taking quizzes." Critical questioning also emerged in relation to geolocation issues more broadly beyond this activity. For example, in response to a news article on a messaging app, Teen 5 began to question how geolocation intersects with privacy policies of corporations. Teen 5 was aware that even though a user may opt out of sharing geolocation data, the IP address may reveal information about one's location:

> I learned that even though the location setting of your phone is off, they can still somewhat track the area you are in. I want to learn how the rules about changing the terms of agreement works. Can you change it whenever you feel like it? Do you have to tell your users that you are changing it? (Teen 5)

The peer researchers' varied responses to the IP Tracer activity and broader codesign workshops showed how consciousness can be developed about critical definitions, such as *personal information*, in privacy legislation like PIPEDA. Other badges in the privacy badges ecosystem, such as the PIPEDA Remixer and Profiler, served to introduce the legislation and the policy actors to youth more directly, and also allowed them to build on their knowledge of policy processes to include political economic understandings of the Internet.

Policy Processes Plus Political Economy

The PIPEDA Remixer and Profiler badges (see Figure 3) continued to engage youth to understand policy processes but also to incorporate political economy considerations. The PIPEDA Remixer badge had youth work in teams to explore a fair information practice from PIPEDA, and to remix and hyperlink short Web pages that shared what they learned about PIPEDA. The Profiler badge had youth remix a template profile page, to share information about an organization or job title relevant to privacy protection in Canada (i.e., the Office of the Privacy Commissioner of Canada, or a privacy officer).

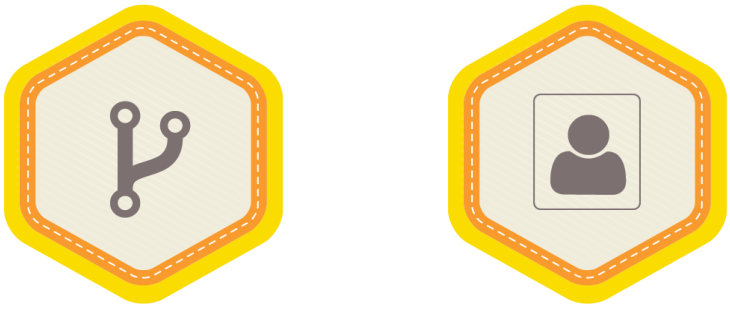

Figure 3. PIPEDA Remixer and Profiler badges.

In terms of generating awareness of policy processes in a way that builds from other activities such as the IP Tracer, the PIPEDA Remixer and Profiler badges worked in tandem. Civics education has long established that citizens need to understand the interlinked components of their governments and the roles of various officials to understand the laws of their country (Kennedy, 1997). In the Canadian context, the House of Commons and Governor General, for example, play intrinsic roles as legislative bills get passed. The PIPEDA Remixer badge encourages exploration of a Canadian bill relevant to privacy, and the Profiler badge encourages awareness of privacy-related offices and roles that are required to uphold the legislation. An educator situated in the civic and legal education sector noted the importance of these kinds of activities in the privacy badges project:

> It's very important to know who . . . these folks are in the systems and what their roles are so you know the proper protocol . . . if you do have . . . issues or complaints or problems or misunderstandings.

Peer researchers from the project team also expressed enthusiasm for the remix activities associated with privacy policy. Teen 1 felt that the PIPEDA Remixer was a particularly important badge in the project: "I have an interest in policy and law, so I think that I've been able to incorporate some of that into the badges" (Teen 1, Minigroup post).

Bringing policy and law to the forefront is one way in which the PIPEDA Remixer and Profiler badges contribute to the political economy considerations of digital policy literacy. In relation to privacy, much attention is focused on the regulatory challenges posed by the commercialized nature of immanent surveillance on the Web (Campbell & Carlson, 2002; Nissenbaum, 2011; Turow, 2011). Yet, although youth who engage in Web search, social networking, gaming, and other online endeavors are subject to immense amounts of commercial surveillance, there also remains an empowerment possibility in using the open Web to learn and share about privacy.

The PIPEDA Remixer and Profiler badges were premised on the use of the open source Mozilla Thimble software tool to remix code (https://thimble.mozilla.org/). Template pages were created for Thimble, which participants could remix by changing the code and then publishing their own versions. The learning activities in the privacy badges curriculum leveraged Mozilla's open source tools, which encourage individuals to become producers and not just consumers of the Web. In this manner, the project demonstrated an engagement with political economic concerns by presenting open source as an alternative to the highly commercialized Internet.

Although open source tools were central to the project, the project also relied on proprietary Web platforms, such as Google Search and Google Docs, to support project participation and collaboration. This lingering tension, between using commercial platforms as part of a project designed to critique the privacy and surveillance implications of the commercial Web, proved productive for discussing political economy with the teen peer researchers. For instance, one peer researcher remarked that the project would not be possible without the Web, including both open source and proprietary tools: "Without the Web, how would we access all our information, or do our research? The Web gave us access to tools such as Mozilla Webmaker, IP tracking websites, Google Maps, and so much more" (Teen 7, Minigroup post). Another peer researcher reflected on some of the strangeness of learning about privacy while using the Web where surveillance is implicit:

> The one thing I do find strange about using the Internet in our peer-research group is that we are researching and learning about privacy and online privacy violations on the very "thing" that robs us of our online privacy. Obviously there are very few corrections to this dilemma, but it seems like a take-two-steps-forward-and-one-back type situation. In conclusion I feel that using the Internet to educate is awesome (due to the interactive learning activities we can partake in), but it has a downside as well, and we need to make sure we take the downside into account every time we type in that search bar. (Teen 8, Minigroup post)

The privacy badges project attempted to make strategic use of the open Web to promote empowerment among youth, but the commercialized Web remained present and even necessary for aspects of the project.

Policy Processes Plus Political Economy and Infrastructures

The peer researchers' reflections concerning open source and corporately owned software as part of the Internet they used for the privacy badges project raises issues relevant to infrastructure from the policy literacy framework. As described by Star (1999), infrastructure is often thought of as "a system of substrates" (p. 380), where there may be limited opportunities for involvement and decision making by lay citizens. In the context of the digitally mediated lives of youth, there are numerous websites and platforms where teens must navigate complex decisions concerning their privacy, but where they have constrained agency because the technologies have largely stabilized.

Accordingly, many infrastructure studies scholars who are interested in the Internet are currently looking at the structural issues and how the Internet works (Sandvig, 2013). Encouraging youth to understand how the Internet works was an implicit and explicit aspect of the privacy badges project. The use of OERs, such as Thimble for website creation and remix, and the open badges infrastructure itself, introduced the idea that there are technology design communities where users are encouraged to participate and be creative.

Although the peer researchers who participated in the project made use of OERs to learn about privacy, they were not necessarily transformed into open source advocates by the end of the project. What did emerge among the youth was an understanding that they could (at least in a limited way) participate in the design of technologies and interrogate how things work to promote greater understandings of privacy. The teens demonstrated an interest in opening the black box of technology. Emanating from Science and Technology Studies, *black box* refers to a technology for which people do not understand the inner workings because only the inputs and outputs are decipherable (Bijker, Hughes, & Pinch, 1987). An example of opening the black box emerged from developing the IP Tracer badge, when peer researcher Teen 7 wanted users of the curriculum to go beyond using websites to look up IP addresses. Teen 7 advocated that learners should use the command prompt or Terminal program to ping for an IP address versus searching through Google or a website with a friendly graphical user interface constructed for the same purpose.

Teen peer researchers also grew to perceive the Internet as a widespread infrastructure for surveillance throughout the project period. Although the privacy badges project began by attending to privacy issues relevant to PIPEDA, such as personal information collection and use by corporations, youth readily found connections to other realms in the post-Snowden era. The youth became aware of increased surveillance of citizens by governments.[5] One of the teens built on what they learned about data collection by corporations and positioned governments as following suit:

> I learned that governments are following the trend of trying to gain more access to personal information. Previously, I knew that governments could obtain warrants and use relatively private Web and phone data for criminal cases and other extreme circumstances. However, I did not know that governments were interested in obtaining more personal data with greater ease. (Teen 1, Minigroup post)

Amid an awareness of the Internet as a surveillance infrastructure, a sense of hopefulness that the peer researchers could continue to impact privacy and be involved in the community also permeated through the project team.

Peer researcher Teen 3 expressed, "I think having the badges project on our resume would help us become a volunteer at any other Hive Toronto organization" (Minigroup post). Teen 3 continued to identify that there were further opportunities for peer researchers to stay involved:

[5] For more information on the Snowden revelations of widespread covert surveillance by the National Security Agency, see the Snowden Surveillance Archive (Canadian Journalists for Free Expression, n.d.).

> If you were interested in Privacy Policy and would like to continue thinking about and making a change toward policy, maybe a career in politics would be right for you. An opportunity that would give you an edge, and that we all could possibly be qualified for is the House of Commons Page Program. (Teen 3, Minigroup post)

Empowerment at the citizenship level was achieved for the peer researchers by tinkering with infrastructures and seeing the various policy and educational avenues required for continued involvement in privacy policy issues.

The Postproject Period: Ongoing Challenges and Possibilities

Although the privacy badges project clearly resulted in an enhanced awareness of policy processes, the political economy of media systems, and infrastructures relevant to digital privacy for the teen peer researchers, there remain ongoing challenges in sustaining the project and expanding its reach. The main sustainability success of the project thus far has been the publication of curriculum on the Hive Toronto website and featuring three activities in the Mozilla Protect Your Data curriculum with a potentially global audience. Mozilla's stewardship of the project ensured that some prototypes developed during through codesign with the youth were widely shared and used.

Although there are clearly individuals who are accessing the curriculum, it remains important to note that end users cannot earn and display their badges digitally at present. Although some of the privacy badges were digitally earnable during a project prototyping phase, an array of barriers remain to making the open privacy badges digitally earnable over the long term to achieve the goals of connected learning. Some of the challenges of the privacy badges project already have been acknowledged in the connected learning literature and in particular by Grant (2014), who reviews the results from 30 badging systems funded through the Badges for Lifelong Learning Competition, held as part of the fourth Digital Media Learning Competition.

As Grant (2014) notes, "assessment is one of the most critical components of a badge system" (p. 33). The first barrier to making the privacy badges available to earn online is the time that is required to evaluate learners' projects before issuing badges. Open badges often require the committed participation of organizations that have assessed the learners' work as part of a long-term process (Goligoski, 2012). For example, if a learner has attempted to earn the Profiler badge, a Hive Toronto staff member, a librarian, or a peer volunteer might be needed to review the Web page a learner constructed to share their knowledge about a privacy-relevant office or profession. The complexities of assessment are also experienced as a challenge in the design of other badging systems, such as the Open Source Nature & Science Badge System (HASTAC, 2013). For the Open Source Nature & Science System, the designers reflect that automated assessment involves a trade-off where assessing engagement (i.e., time spent at a computer-based activity station) is often more feasible than assessing the quality of learning (HASTAC, 2013).

In addition to designing for appropriate assessment, open badges must be credible: "making that learning visible is the core purpose of open digital badges since they provide a credible way to

communicate learning to others" (Grant, 2014, p. 11). Goligoski (2012) cautions that distributed assessors may introduce uncertainty into a badge's accreditation function. For example, if a youth earned the IP Address Tracer badge, who would see the learning as valuable? Would an after-school program recognize the skills gained in relation to a preexisting computing certificate? Would a postsecondary scholarship provider be comfortable recognizing a youth's effort to earn the badge as an extracurricular activity? Grant (2014) argues that open badges challenge organizations to create new pathways for youth to expand their opportunities. Creating the organizational collaborations to support such learning pathways could not be fully achieved in our privacy badges project time frame.

Another challenge of open badges comes from their significance to learners, which can be dependent on specific contexts for learning. Some of the early adopters of open badges are educational institutions (see Abramovich, Schunn, & Higashi, 2013; Gibson, Ostashewski, Flintoff, Grant, & Knight, 2015; Glover & Latif, 2013). In a study of the ways educators and learners responded to the introduction of open badges in a postsecondary setting, Glover and Latif (2013) found that although most reactions to badges were positive, implementation required significant changes to the general perception of badges' credibility and value for learners. From the point of view of students, badges could function as an extrinsic motivator, but only if there were some links between earning a badge and demonstrating more than simply a baseline level of engagement. For example, Glover and Latif suggest the creation of "special badges" that would enable high achievers to stand out from their peers. Similarly, Gibson et al. (2015) note that badges afford status recognition and learners may seek desirable outcomes such as getting a job. Such research indicates how the status of badges as a mark of learning is reliant on the specific learning situation and is still relatively uncertain.

These kinds of assessment and credibility challenges in the privacy badges project were also complicated by the flux in leadership for the open badges infrastructure during and after the project. Mozilla was a key player in the open badges infrastructure when the privacy badges project was first proposed, but its role changed over time. As described in a Mozilla blog post (Surman, 2016), a network called the Badge Alliance launched in 2014 to support the development of the ecosystem for open badges and other organizations, such as Digitalme, are currently contributing to open badges' technical infrastructure (Riches, 2016). Given that only a relatively small array of organizations in Canada have implemented open badges thus far,[6] it proved difficult to attract collaborators and partners to sustain the privacy badges while still in the prototype stage.

More generally, the uneasy intersection between accreditation and gamification that open badges represent has further been critiqued by a number of commentators, who note that the extrinsic rewards conferred by badging may reduce the intrinsic motivation that youth have for learning (reviewed in Goligoski, 2012). Furthermore, such a motivation gap might take shape along an accessibility divide between organizations and educational institutions that do not all share the same access to resources for badge implementation. Again, the issue of long-term organizational, community, and institutional support for badges manifests as a crucial challenge to the future of the open badges program.

[6] Organizations in Canada that have implemented open badges include the Boys & Girls Clubs of Canada, University of British Columbia, and a Quebec-based distance education college (Cégep à distance).

Conclusion

The privacy badges project incorporated ideas from connected learning, privacy as contextual integrity, networked privacy, and empowerment approaches to privacy to encourage youth to codesign OERs suitable for themselves and their peers. This research approach was intended to counter educational initiatives that position youth primarily as data subjects who need to be taught not to disclose their personal information (see Steeves, 2010). The privacy badges project successfully demonstrates that teen codesigners can develop digital policy literacy through relevant insights about privacy policy, the political economy of the Internet, and digital infrastructures, while prototyping a privacy badges ecosystem. Fostering opportunities for youth to explore privacy and to enhance it through codesign is critical for the creation of successful educational resources. Researchers, adults, and informal learning organizations cannot realistically design appropriate privacy education initiatives without involving youth by integrating their perspectives and contributions.

The privacy badges project was fortunate in that research funding from the Office of the Privacy Commissioner enabled partners including Mozilla, Hive Toronto, and a local university to create an opportunity that was appealing to youth. The academic research staff perceived that the youth were motivated to participate not only to gain experience with Mozilla, a well-known software organization, but that being rewarded for their participation through gift cards as an honorarium was an incentive. Recognition for every hour of project participation was critical to create a dynamic in which youth were recognized as collaborators and codesigners.

Although the openly licensed teaching activities and prototyped badges from the project are a success, further challenges remain in extending the reach of the project to other youth beyond the codesign team. Convening an array of organizations that will use, issue, and assess the privacy badges within the broader open badges community requires ongoing effort and resources. In the interim, the simple availability of the learning activities and prototype badges offers educational opportunities relevant to the digital policy literacy framework. As the badges become incorporated in other learning settings, we recognize that it is unlikely that youth will have the extended six-month opportunity to engage with policy, political economy, and infrastructure issues in an identical manner to that of the peer researchers. To best emulate the experience of the peer researchers, we recommend the implementation of multiple badges from the ecosystem wherever possible. We also encourage the use of open Web infrastructures as a critical step to encourage increased understanding and engagement with the policy processes and political economy considerations that are relevant to privacy in the networked lives of youth.

References

Abramovich, S., Schunn, C., & Higashi, R. M. (2013). Are badges useful in education? It depends upon the type of badge and expertise of learner. *Educational Technology Research & Development, 61*, 217–232.

Agre, P. E., & Rotenberg, M. (1998). *Technology and privacy: The new landscape*. Cambridge, MA: MIT Press.

Amichai-Hamburger, Y., McKenna, K. Y. A., & Tal, S. A. (2008). E-empowerment: Empowerment by the Internet. *Computers in Human Behavior, 24,* 1776–1789.

Atkins, D. E., Brown, J. S., & Hammond, A. L. (2007). A review of the open educational resources (OER) movement: Achievements, challenges, and new opportunities. Retrieved from http://www.hewlett.org/wp-content/uploads/2016/08/ReviewoftheOERMovement.pdf

Belshaw, D., Smith, K. L., & the Mozilla Community. (2014). Why Mozilla cares about Web literacy. Retrieved from https://mozilla.github.io/webmaker-whitepaper/

Bijker, W. E., Hughes, T., & Pinch, T. J. (Eds.). (1987). *The social construction of technological systems: New directions in the sociology and history of technology*. Cambridge, MA: MIT Press.

Bowker, G. (1994). Information mythology and infrastructure. In L. Bud-Frierman (Ed.), *Information acumen: The understanding and use of knowledge in modern business* (pp. 231–247). London, UK: Routledge.

boyd, d. (2012). Networked privacy. *Surveillance & Society, 10*(3/4), 348–350.

Campbell, J. E., & Carlson, M. (2002). Panopticon.com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media, 46*(4), 586–606.

Canadian Journalists for Free Expression. (n.d.). Snowden surveillance archive. Retrieved from https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi

Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. *Journal of Educational Multimedia and Hypermedia, 13*(1), 93–106.

European Parliament. (2013). Parliamentary questions, 12 March 2013: Answer given by Mrs. Reding on behalf of the commission. Retrieved from http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2013-000873&language=EN

Gibson, D., Ostashewski, N., Flintoff, K., Grant, S., & Knight, E. (2015). Digital badges in education. *Education and Information Technologies, 20*(2), 403–410.

Glover, I., & Latif, F. (2013, June). *Investigating perceptions and potential of open badges in formal higher education*. Paper presented at the World Conference on Educational Multimedia, Hypermedia and Telecommunications, Chesapeake, VA.

Goligoski, E. (2012). Motivating the learner: Mozilla's open badges program. *Access to Knowledge: A Course Journal, 4*(1), 1–8.

Grant, S. L. (2014). *What counts as learning: Open digital badges for new opportunities*. Retrieved from https://dmlhub.net/publications/what-counts-learning/

Halavais, A. M. C. (2011). A genealogy of badges: Inherited meaning and monstrous moral hybrids. *Information, Communication & Society, 15*(3), 354–373.

HASTAC (Humanities, Arts, Science, and Technology Alliance and Collaboratory). (2013). Project Q&A with: NatureBadges: Open Source Nature & Science Badge System. Retrieved from https://www.hastac.org/wiki/project-qa-naturebadges-open-source-nature-science-badge-system

Ito, M., Gutiérrez, K., Livingstone, S., Penuel, B., Rhodes, J., Salen, K., . . . Watkins, S. C. (2013). *Connected learning: An agenda for research and design*. Irvine, CA: Digital Media and Learning Research Hub.

Jenkins, H., Ito, M., & boyd, d. (2015). *Participatory culture in a networked era: A conversation on youth, learning, commerce, and politics*. Malden, MA: Polity.

Kellner, D. (2002). New media and new literacies: Reconstructing education for the new millennium. In L. Lievrouw & S. Livingstone (Eds.), *The handbook of new media* (pp. 90–104). London, UK: SAGE Publications.

Kennedy, K. J. (1997). *Citizenship education and the modern state*. London, UK: Falmer Press.

MacArthur Foundation. (2010). Digital media and learning competition [Press release]. Retrieved from https://www.macfound.org/press/press-releases/digital-media-learning-competition/

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society, 16*(7), 1051–1067.

Meyers, E. M., Erickson, I., & Small, R. V. (2013). Digital literacy and informal learning environments: An introduction. *Learning, Media and Technology, 38*(4), 355–367.

Montgomery, K. C. (2015). Youth and surveillance in the Facebook era: Policy interventions and social implications. *Telecommunications Policy, 39*(9), 771–786.

Mozilla. (2015, July 14). Mozilla's Maker Party starts today [Blog post]. Retrieved from https://blog.mozilla.org/blog/2015/07/14/mozillas-maker-party-starts-today/

Mozilla. (n.d.). Web literacy. Retrieved from https://learning.mozilla.org/en-US/web-literacy

Mozilla Clubs. (n.d.). Design thinking. Retrieved from https://learning.mozilla.org/en-US/web-literacy

Mozilla Hive New York. (n.d.). Timeline. Retrieved from http://hivenyc.org/about-hive-nyc/timeline/

Mozilla Open Badges. (n.d.). Get recognition for skills you learn anywhere. Retrieved from https://web.archive.org/web/20160324221138/http://openbadges.org:80/

Muller, H., Timmermann, J., Fortmann, J., Heuten, W., & Boll, S. (2013, August). *Proximity sensor—Privacy aware location sharing*. Paper presented at the Mobile HCI, Munich, Germany.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 101–139.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Dædalus, 140*(4), 32–48.

Office of the Privacy Commissioner of Canada. (2013). What an IP address can reveal about you. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/

Rafalow, M. H., & Larson, K. (2014). *Fashioning learning: Connected learning through fashion design programs*. Irvine, CA: Digital Media and Learning Research Hub.

Raynes-Goldie, K. (2010, January 4). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1).

Raynes-Goldie, K., & Allen, M. (2014). Gaming privacy: A Canadian case study of a co-created privacy literacy game for children. *Surveillance & Society, 12*(3), 414–426.

Regan, P. M., & Steeves, V. (2010). Kids R Us: Online social networking and the potential for empowerment. *Surveillance & Society, 8*(2), 151–165.

Rich, J. (2016). Keeping up with the online advertising industry [Blog post]. Retrieved from https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry

Riches, T. (2016). Backpack to the future [Blog post]. Retrieved from https://medium.com/digitalme-an-open-badge-adventure/backpack-to-the-future-eb66c5c67d5a

Sanders, E. B. N., & Stappers, P. J. (2008). Co-creation and the new landscapes of design. *CoDesign, 4*(1), 5–18.

Sandvig, C. (2013). The Internet as infrastructure. In W. Dutton (Ed.), *The Oxford handbook of Internet studies* (pp. 1–27). Oxford, UK: Oxford University Press.

Santo, R., Ching, D., Peppler, K., & Hoadley, C. (2016). Working in the open: Lessons from open source on building communities of educational innovation. *On the Horizon, 24*(3), 1–36.

Schuler, D., & Nakioma, A. (Eds.). (1993). *Participatory design: Principles and practices*. Hillsdale, NJ: CRC Press.

Shade, L. R. (2015). I want my Internet! Young women on the politics of usage-based billing. In J. Bailey & V. Steeves (Eds.), *eGirls, eCitizens* (pp. 411–434). Ottawa, Canada: University of Ottawa Press.

Shade, L. R., & Shepherd, T. (2013, December 2). Viewing youth and mobile privacy through a digital policy literacy framework. *First Monday, 18*(2).

Smith, K. L., & Belshaw, D. (2015). Exploring net neutrality with Mozilla Webmaker. Retrieved from http://civicmediaproject.org/works/civic-media-project/netneutralitymozillawebmaker

Smith, K. L., Meisner, K., Shade, L., Shepherd, T., & Belshaw, D. (2015). Co-designing open badges for privacy education with Canadian youth. Retrieved from http://hivetoronto.org/wp-content/uploads/2014/09/CoDesigningBadgesFinalReport-30March2015.pdf

Star, S. L. (1999). The ethnography of infrastructure. *American Behavioral Scientist, 43*(3), 377–391.

Steeves, V. (2010). *Summary of research on youth online privacy*. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2010/yp_201003/#wb-cont

Surman, M. (2016). Mozilla's continued commitment to open badges [Blog post]. Retrieved from https://learning.mozilla.org/blog/mozillas-continued-commitment-to-open-badges

Turow, J. (2011). *The daily you: How the new advertising industry is defining your identity and your worth*. New Haven, CT: Yale University Press.

Tyner, K. (1998). *Literacy in a digital world: Teaching and learning in an age of information*. Mahwah, NJ: Erlbaum.

Vickery, J. (2015). "I don't have anything to hide, but . . . ": The challenges and negotiations of social and mobile media privacy for non-dominant youth. *Information, Communication & Society, 18*(3), 281–294.

World Economic Forum. (2012). *From consumers to creators: Empowering the digital*. Retrieved from http://www3.weforum.org/docs/WEF_ITTC_ConsumersCreatorsEmpoweringDigitalGeneration_Report_2012.pdf