Leslie Regan Shade and Tamara Shepherd

Viewing youth and mobile privacy through a digital policy literacy framework

Article (Published version)
(Refereed)

http://eprints.lse.ac.uk

f i ® s t m ¤ ñ d @ ¥
PEER-REVIEWED JOURNAL ON THE INTERNET

Viewing youth and mobile privacy through a digital policy literacy framework
by Leslie Regan Shade and Tamara Shepherd

Abstract
Digital policy literacy is a critical element of digital literacy that emphasizes an understanding of communication policy processes, the political economy of media, and technological infrastructures. This paper introduces an analytical framework of digital policy literacy and illustrates it with examples of young people's everyday negotiations of mobile privacy, in order to argue for increased policy literacy around privacy and mobile phone communication. The framework is applied to the Canadian context, where a small pilot study engaged 14 undergraduate university students in focus groups about their uses of mobiles and knowledge of mobile privacy issues. Preliminary findings show that while our participants were aware of a variety of privacy threats in mobile communication, they were not likely to participate in policy processes that might protect their privacy rights. The paper concludes with a discussion of why young people may not be motivated to intervene in policy processes and how their digital policy literacy around mobile privacy is mitigated by the construction of youth as a lucrative target consumer market for mobile devices and services.

Contents

Introduction

> I think it's pretty obvious that it's coming to a point where you don't really have any privacy ... And it's been that way, it's just more visual now, we know more about it. I don't know whether that's because we're older now and we discuss it. Because I'm sure they've always had access to our information, it's just that it's been more important, depending on what age category you are. Like they can't really target everything toward you when you're 17. (Stephanie, third–year undergraduate) [1]

This comment from a focus group participant reflects the often–cynical attitude of young Canadians toward mobile phone marketing practices and their understanding of privacy challenges in mobile communication. In this paper, we ask how young people understand and negotiate their mobile privacy, situating it within a framework of digital policy literacy. This framework enables us to unpack the interrelated dimensions of policy processes, the political economy of media systems, and the infrastructures of communication systems, as they impinge on young Canadians' mobile privacy. Privacy in mobile environments is an important regulatory concern, especially for young people who eagerly adopt networked mobile applications that can compromise their informational privacy. The digital policy literacy framework thus works to orient the discussions with young Canadians about their mobile privacy so they can better understand, and take action to intervene in, policy–making that recognizes privacy rights as integral to participation in a digital society.

Situating digital policy literacy

Canadian federal policy on the digital economy frames digital literacy initiatives as a crucial site for training youth in digital skills, defined as 'the ability to locate, understand, evaluate, create and share information using digital technology' [2]. Fluency in digital practices constitutes not only the basis for a thriving information economy, but enables a more connected and engaged citizenry; increased digital literacy will 'open up new opportunities for all Canadians to participate in Canada's democratic, economic, cultural and social life' [3].

In their submission to Industry Canada's Digital Economy Strategy Consultation, the media literacy organization Media Awareness Network (now renamed MediaSmarts) argued for a comprehensive national digital literacy plan involving government, civil society, and educators, to strengthen the Canadian economy and enhance Canadian lives (Media Awareness Network, 2010). Based on a survey with diverse stakeholders, the Canadian Internet Registration Authority (CIRA) positioned digital literacy — encompassing use, understanding, and creation of digital media content and technologies — as essential for achieving the 'digital economy value chain' of creativity, innovation, productivity, and competitiveness [4].

These examples illustrate how digital literacy is promoted as essential for Canadian youth in an increasingly technologically mediated society. Missing from these entreaties for digital literacy, however, is an explicit focus on the acquisition of knowledge about digital policy issues. Rather than being an essential component of digital literacy, digital policy issues are mentioned with reference to the mitigation of risks and to protect youth from harm by, for instance, averting online identity fraud or enhancing reputation management. Intellectual property policy is evoked so that youth can better understand what constitutes copyright infringement in order to dissuade piracy practices. In relation to privacy, regulatory development of tools for young people to protect their online privacy tend to focus on cultivating skills of individual information disclosure (*e.g.*, the Office of the Privacy Commissioner of Canada's Youth Privacy portal), and the deliberate use of software featuring "privacy by design" principles (*e.g.*, Ontario Information and Privacy Commissioner Ann Cavoukian's promotion of built–in privacy protections) [5].

We argue that regulators' focus on digital skills, and attendant discussion of policy only insofar as it addresses business issues such as fraud, piracy, and liability, obscures a consideration of the democratizing possibilities of digital literacy for civic participation (O'Neill and Hagen, 2009). Public discourse about digital literacy tends to frame youth as mere consumers. We concur with O'Neill, who contends that this focus on ethical individualism needs to be countered with an alternative vision foregrounding communication rights that would consider 'the right to accessible information, the right to communicate and the right to privacy' [6]. The digital policy literacy framework adds this crucial conception of rights to prevailing models of digital literacy.

A focus on communication rights directs attention to new challenges for literacy and pedagogy. Within communication policy research, digital literacy is said to be 'gaining ascendancy, in key ways taking over the ground where audience studies once held sway' (Livingstone, 2008). Digital literacy typically refers to the technical, cognitive, and sociological skills needed in order to perform tasks and solve problems in digital environments (Tyner, 1998). Notions of digital literacy can be traced to earlier accounts of 'computer literacy' in the 1980s (Bawden, 2001), and 'information literacy' in the 1990s (Behrens, 1994). By situating digital literacy as primarily comprising technical skills, the vestiges of the computer and information literacy approaches remain, most recently framed as the '21st century skills' required for participation in a high–tech economy (Trilling and Fadel, 2009).

Alongside these instrumental versions of literacy in technological environments, critical variations of digital literacy draw from media literacy approaches concerned with the pedagogical impact of digital media in society (Alvermann and Hagood, 2000; Hobbs, 2011). Here digital literacy challenges notions of skills procurement; Buckingham, for example, describes how digital literacy cannot be seen 'simply as a matter of "information" or of "technology,"' but as a means of 'cultural understanding' [7], which involves a critical perspective on the social, political, and economic implications of the ubiquity of information technology. This stance is furthermore intended to foster in young people critical analysis of the relationships between media and audiences, information and power, as a crucial element of participatory democracy in the twenty–first century (Kellner and Share, 2007; Livingstone and Brake, 2010; Hoechsmann and Poyntz, 2012).

The digital policy literacy framework

Digital policy literacy is aligned with critical approaches to digital literacy, and emphasizes how the effective use of digital media involves learning and negotiating the policy processes, political economic parameters, and infrastructural affordances that shape technologies. The framework suggests that while young Canadians are often astute users of digital media technologies — incorporating them as central tools in their everyday roles as students, friends, employees, job seekers, and cultural creators (Shade, 2012) — they also face potentially exploitative rights structures in digital environments, for example in relation to media access, content, intellectual property, and privacy online (Hamilton and Pors, 2003; Shepherd, 2012). It is important for

young people to become more knowledgeable about digital policy issues in an increasingly complicated corporate context for protecting user rights. As such, we argue that the digital policy literacy framework is a crucial addition to existing skills–based conceptions of digital literacy, in that it contributes an urgent consideration of the role of policy in everyday networked communication. The framework is constituted by three main elements:

1. Policy processes

This element of digital policy literacy involves an understanding of how policy is created, particularly the governance of communication resources at local, national, and global levels. What policy issues appear on the agenda, how they are constituted, and the shaping of participation in policy processes are key aspects. The structural contours of policy processes include specific institutions of policy governance, diverse formal and informal mechanisms for public participation, and the roles allocated to diverse stakeholders in particular policy contexts (Freedman, 2008; Galperin, 2004; Napoli and Aslama, 2010). These structures both enable and constrain citizen and youth involvement in making policy decisions around digital communication. Effective modes of policy activism and intervention within, or outside of, official policy–making processes are also key.

2. Political economy of media systems

Understanding the broader social and political relations surrounding the ownership, production, distribution, consumption, and creation of media is the second element of digital policy literacy. The political economic considerations shaping digital media and communication include an analysis of media industries and institutions, the changing contours and politics of media ownership, and the interaction between mainstream and alternative or independent media (McChesney, 2013; Mosco, 2009). Media systems reinforce, challenge, and influence social relations, and impact how citizens are represented and included (or excluded) from policy decisions on issues that tangibly affect their lives and livelihoods.

3. Infrastructures

Infrastructures can be thought of as a socio–technical system. In the case of mobile infrastructures, we can envision them as encompassing the technical infrastructures of operating systems — software that manages the hardware of mobile devices, their operating features, and related applications such as location–based devices. There are also knowledge infrastructures of informational and communication systems governed by standards, operating procedures, and international governance regimes (Bowker, *et al.*, 2010).

The relationship between policy and infrastructure development is long established, especially in the context of Canada's vast geographical area and relatively sparse population (Charland, 1986; Barney, 2005). But in addition to literacy about how policy decisions shape communications infrastructure, the more general questions to ask of communication technology infrastructures include: how does the design of digital communications systems, devices, and networks affect everyday online interactions? What are the affordances of technology design in terms of content, including the ownership of digital content? How might infrastructural parameters impinge on personal privacy management? What are the often–invisible values built in to technological artifacts produced under certain regimes of power? A social justice perspective on the role of policy in determining infrastructural affordances is crucial to these questions.

Through the three elements — policy processes, political economy of media systems, and infrastructures — the digital policy literacy framework addresses the imperative for expanded notions of literacy beyond the facile notion of 'how to use' digital technologies, as described in the information literacy paradigm that informs Canada's digital economy strategy (Whitehead and Quinlan, 2002). Moving beyond simplistic and individualistic emphases on 'digital skills,' the digital policy literacy framework underscores how skills are shaped by a larger social and political context around digital media technologies.

The digital policy literacy framework may be applied to a number of socio–political contexts around digital technology and youth. An enduring concern about digital technology is access for social inclusion (Park, 2012), to which the digital policy literacy framework adds literacy about how access is determined by a range of institutional factors, including the governance of information architecture.

While access is a key concern for young people entering into civic life through digital technology, the flip side of this access is risk and harm, evidenced by moral panics about harmful digital content, online predators, and youth sexuality (*e.g.*, boyd, *et al.*, 2011; Draper, 2011). The framework can put these issues into perspective, for instance by situating legislation like the U.S. Children's Online Privacy Protection Act (COPPA) within broader debates around the status of youth rights and the public interest (Finkelhor, 2010).

Typically reflecting corporate as opposed to public interests, the status of digital content as intellectual property can be seen through the digital policy literacy framework in terms of how legal and regulatory copyright mechanisms may support commercial imperatives (Palfrey, *et al.*, 2009; Gillespie, 2007).

Finally, issues around digital privacy are urgent to examine from the digital policy literacy

perspective, as new technological innovations usher in increasingly sophisticated regimes of surveillance (Marx and Steeves, 2010; Raynes–Goldie, 2010). The following section illustrates the digital policy literacy framework by addressing how it relates to the issue of youth and privacy in mobile technologies.

Illustrating the framework: Canadian youth and mobile privacy

One context where we have begun to apply the digital policy literacy framework is that of young Canadians' everyday negotiations of informational or data privacy in mobile communication. Through a pilot study that comprised a series of interviews and focus groups with 14 youth aged 18–25 who were students at a large, urban Canadian university in 2011 and early 2012, we sought to understand how digital policy literacy might fit into the kinds of learning that these young people were already engaged in around online privacy, relating to their use of mobile phones. There were four focus groups and two interviews conducted, wherein several scenarios were presented to the participants in order to guide the discussion. Scenarios focused on different kinds of mobile privacy (etiquette and situational, social privacy and security, internet connectivity and data privacy, and locational privacy). Participants were also queried about their concerns around corporate or government surveillance and what sorts of privacy education should be made available for young people.

We used this method in order to generate discussion about how mobile privacy is perceived by individuals and in–group settings, and as a way of revealing prevalent social norms around privacy literacy. It is important to note that while this group of youth served as a revealing sample population in terms of their status as a targeted demographic for mobile devices and applications, undergraduate students tend to be an over–studied population in this regard. In developing this program of research on youth and mobile privacy, we aim to recruit young people from secondary schools and those outside of university settings.

For this pilot study, the participants were asked to reflect upon the intersections between the digital policy literacy framework and their typical experiences of mobile communication. We aimed to orient the discussion around questions such as: how were these young people's everyday experiences of privacy in mobile environments shaped by policy processes, the political economy of media systems, and infrastructures? What were their concerns about mobile data privacy? How did they negotiate mobile privacy, both on their own in everyday practices, and possibly through policy and activist channels? How did they seek out more information about their privacy rights in relation to mobile technologies?

Given the centrality of the mobile phone for young people, their understanding and negotiation of mobile privacy is important. According to a survey conducted for the Canadian Wireless Telecommunication Association, 18–24–year–olds are the consumer group with the highest levels of mobile device adoption (Quorus, 2012). Recent findings from the Pew Research Center's Internet and American Life Project show that for typical teens and young adults, mobile phones are an essential channel of communication, particularly for texting and taking pictures (Lenhart, 2012; Duggan and Rainie, 2012). In addition to their utility for communication and expression, mobile devices facilitate identity formations within different contexts (Stald, 2007). At the same time, mobile devices engender feelings of security among both young people and their parents while also complicating the negotiation of familial communication, trust, and autonomy (Clark, 2013; Turkle, 2011).

Yet, while mobile devices serve a number of practical and symbolic functions in relation to young people's safety, they elicit new safety concerns. For instance, the safety net provided by mobile phones is often illusory, particularly given the trade–offs of familial surveillance supported by the devices and the prevalence of cyberbullying via mobiles [8]. Moreover, the surveillance and security issues raised by mobile devices are not constrained to local social contexts; institutional actors, including governments and corporations, have unprecedented access to the location–based information of mobile device owners (Shilton, 2009). This surveillance architecture invites threats to mobile informational or data privacy, that is the privacy of personally identifying information as it is collected, bought and sold through marketing practices [9].

Informational privacy is our main concern in this study, even though most research to date on mobile privacy assesses social privacy, or the disclosure of information to other individuals (*e.g.*, Jeffery, 2008; Mancini, *et al.*, 2009; Nippert–Eng, 2010). For younger users of networked technologies, social privacy threats tend to be the locus of academic research (Marwick, *et al.*, 2010). Social privacy concerns may be more immediate for younger users of networked technologies, who have been shown to be less aware than adults of privacy threats posed by marketing practices in social network sites, immersive online environments, and networked games (Lawford, 2008; Steeves and Webster, 2008; Grimes and Shade, 2005).

However, a more recent study finds that young people's intrepid use of social network sites is tempered by their consciousness of surveillance practices emanating from their schools, parents, or corporate sites (MediaSmarts, 2012). Mobile technology poses similar privacy threats to young users, with the addition of sensitive location–based data that undermines the anonymization of

personal information (Beach, *et al.*, 2009; Urban, *et al.*, 2012). And yet, to date there remains a lack of extensive scholarly research on the intersection of youth privacy and mobile privacy. As Goggin (2013) argues, research on mobiles and youth needs to engage with issues that are crucial to contemporary public policy debates. Given the heightened concerns surrounding threats to young people's mobile privacy, the digital policy literacy framework is an apt lens through which to understand how the young people in this pilot study described their negotiations of mobile privacy.

1. Policy processes

The first element of the framework, policy processes, is concerned with how mobile privacy is situated within the federal policy agenda. In Canada, the agency most active in privacy policy is the Office of the Privacy Commissioner (OPC). The OPC has produced significant research and outreach around youth privacy, noting the increased use of mobile devices for social networking, where location data and personal information can be collected through mobile apps [10]. It has further asserted that Canadian mobile advertising campaigns should require mobile users to opt in to location–based services rather than opt out [11]. On the technology side, the OPC has created a best practices guide for mobile app developers, admonishing them to consider user privacy as 'a key competitive advantage' [12], while also itself launching the myPRIVACYapp, a mobile application available for several platforms that educates users on how to better protect their personal information on mobile devices (OPC, 2013). These examples illustrate how the work of the OPC is often agenda–setting and situated among other recent privacy initiatives and studies in the U.S., notably those conducted by the Federal Trade Commission and the Pew Research Center's Internet & American Life Project [13].

Yet despite its considerable research and outreach activities, the influence of the OPC on legislative decisions is limited. Working independently of other government agencies, primarily via investigating privacy complaints, the OPC's impact is through the expert provision of legal and policy analyses for Parliamentary legislative review. Because such policy–making lags behind rapid technological change, privacy in mobile social media apps is now regulated solely by corporate terms of service and privacy policies.

Assumptions about young people's lack of concern for privacy underlie many privacy–threatening mobile applications, illustrated for example in Facebook CEO Mark Zuckerberg's infamous claim in 2010 that privacy was no longer a 'social norm' (Johnson, 2010). But as Steeves remarks, these assumptions are unfounded: 'In fact, if you look at the empirical evidence, all the research indicates that privacy is absolutely essential to tweens, to teenagers, and to young adults. And that they're very conscious of negotiating that line between their privacy and their public performances' (Steeves, in Cucinelli and Shade, 2012).

1.1. Understandings of mobile privacy

In our focus groups and interviews, young people appeared savvy about their informational mobile privacy; they are aware that information, including location data, is constantly being collected from their devices. For example, JA said, 'I know Apple collects it, but that bothers me less [... than] Facebook apps or browser extensions that just take everything you have and then share it — that's a whole other story.' The collection of information through social network sites on their computers and laptops was perhaps more of a concern for some participants, but as Stephanie noted, smartphones bring social media to the mobile device:

> I feel like absolutely the day I got a smartphone, it was just a whole new world, because at that moment in time, I surrendered to the commercial world, because it was just like, now at that point, you have your Facebook, you have everything. [...] It's like a little computer, right? [...] It's crazy. So I think that when you sign your contract with your phone company, your provider, you're basically just signing away — just bring on the merchandise and the marketing.

Yet while these young people are aware that data is collected through mobile applications, they simultaneously felt that signing up to use these services — described as useful — served as a type of consent for data collection. As Lucas said, 'you don't think about that at all when you use Facebook — you're not thinking of yourself as like a commodity for them'. However, he recognized that the service was 'socially really good: [...] I play in a band and it's important to be promotionally really on top of all of that stuff. You can't do that without a Facebook account.' Moreover, JA added that a certain level of data collection and usage in marketing practices was acceptable, but excessive tracking might put companies' brand integrity at stake. He used the example of Apple, which collects user data through the iPhone's OS, but not too intrusively, since 'it would hurt their brand more than anything else.' He contrasted this against the social app PATH, which 'secretly uploaded your entire address book to its servers,' and was subsequently shut down by the FTC [14].

1.2. Privacy through obscurity

Our focus group discussions revealed that mobile data collection could be troubling. Most of the

time, however, data collection is invisible and ubiquitous, and so the participants claimed that they don't really think about it. Rather than being protected by privacy legislation, our participants felt that they were protected by obscurity. As Amy said, 'I feel like because they have so much information, like, they have everyone's information, I guess I feel better about being one in the millions.' Wallis concurred, 'it doesn't bother me as much, it's just the way the advertising and consumer world works.'

These statements about mobile data collection indicate that such practices are a taken–for–granted element of contemporary networked life. Although our participants sometimes worried about excessive data collection, most of the time the information collected, such as IP addresses, seemed 'not as personal' when it is aggregated, and as Wallis opined: 'There's so many other things that you're thinking about and worried about online. And I feel like that's just like, ok, well really I'm not going to spend the time making sure that these market research[ers] don't really know what I want.' Both through obscurity and the relative lack of harm perceived by these young people, data collection and profiling through mobile devices was not typically experienced as an urgent privacy concern.

1.3. Ambivalence toward data collection

Overall, because our participants expressed ambivalence about mobile data collection, it is difficult to translate their behaviors and attitudes into concrete policy processes, such as youth mobilization through traditional civic channels and consultations. Taking action to protect privacy through commercial structures of privacy policy, however, was something that participants did report engaging in. As JA noted about data collection through mobile apps, 'I try to opt out of it as much as I can,' but that some apps ask users to opt out and some don't: 'it makes me feel more like "meh" about it.' Similarly, Vicky said that she feels as long as the marketing practices are somewhat transparent, she is mostly comfortable with data collection:

> I'm pretty, like whatever. As long as I'm aware of it — you
> know, if I was blind to it, and then like taken advantage
> of, I think I'd be mad. But because I'm open to it and I've
> been taught about it in so many ways, and I've learned to
> protect myself in so many ways, I think it kind of evens it
> out. It's not like they're sneaking around behind my back.
> I know that they're targeting these advertisements to me,
> so it's ok.

Our participants displayed an implicit trust that marketers would not do anything explicitly harmful with their information, and this is mainly why they felt ambivalent about data collection, even though the idea of being tracked could be 'creepy.' As Bianca summarized, 'Well, I think when you buy into the system, if you read the fine print they tell you. [...] You kind of have to weigh it out: do I want to be tracked by this and get the service? Or do I want my privacy?'

These examples from our focus groups and interviews suggest that getting involved in more traditional policy processes, such as public consultations or regulatory hearings, will be a difficult gap for young people to bridge, unless threats to their privacy from mobile applications become exacerbated and blatantly harmful. Consistent with other research on youth and social media privacy (*e.g.*, boyd and Hargittai, 2010), it seems more likely that young Canadians will take smaller, everyday actions to protect their informational privacy on mobile devices through negotiating their uses of certain apps, or by opting out of services such as location–aware features.

2. Political economy of media systems

The political economy of media systems, in this case, the wireless industry in Canada, constitutes the second element of the framework. The Canadian wireless industry is dominated by three established telecommunications giants: Rogers Communications, Inc.; BCE's Bell Mobility, Inc.; and Telus Communications Company. These 'big three' players account for 95 percent of the Canadian market and enjoy the highest profit margins of any wireless corporations in the developed world (Nowak, 2010). The average revenue per user for Canadian carriers is among the highest in the world, and coincides with high costs of service (OECD, 2011).

One of the first steps to improving the often–prohibitive prices of mobile service by increasing market competition has been through wireless spectrum license auctions. Yet, in the series of auctions held since 2008, new entrants have been prevented from fully competing with the incumbent service providers due to the upfront capital required to purchase spectrum licenses and current restrictions on foreign ownership (Longford, 2011).

2.1. Continued lack of competition in Canada's wireless industry

Spectrum auctions have failed to provide a solution to the lack of competitiveness in Canada's wireless industry. Accordingly, our participants described the lack of market competition as a key factor in their frustration with the 'big three' structure of Canadian mobile service provision. Michelle remarked that, since 'everyone hates Bell,' she left the company for one of its subsidiaries, Virgin Mobile, which seemed to have more simplified plans but still lacked clarity in its billing structure: 'It seemed more accessible and easy. It's all right, but it's not great ... the

charge for receiving calls] seems like it's constantly changing; I feel like we never really know what's actually happening.' Similar manipulative billing practices were experienced by Véronique, who used Rogers because of their introductory three–month unlimited plans for the iPhone: 'So you get used to being everyday on the Internet, and then you get your habits, and then Surprise! Month number 4, like, oh my god.' With Telus, Lara had likewise felt that the company misled her with the promise of unlimited service when she selected her five phone numbers for the My5 unlimited calling plan. Only after she had used that plan for a month, and incurred additional charges, did Lara discover that the My5 plan didn't extend outside of Canada: 'That screwed me over. [...] They cheated me.' This expression of mistrust was common among the young Canadians we spoke with (see Shepherd and Shade, 2012).

What the participants shared with us has since been echoed on a larger scale in the public consultation conducted by the Canadian Radio–television and Telecommunications Commission (CRTC) to develop a mandatory Wireless Code for Canada's wireless service providers. In December 2012, the CRTC solicited interventions and public comments about best practices for wireless services and contracts, through a dedicated Web site for submissions and via the CRTC regulatory mechanisms for interventions. The response from a diverse group of constituents, including industry, public interest groups, academics, and especially the general public, was overwhelming. Over 3,500 written comments and 600 online submissions detailed the unfair consumer practices of Canada's 'big three' telecommunication companies (CRTC, 2013).

As Lubomir aptly summarized in our focus groups: 'People only talk about it if they're complaining; there's nothing good to say about it.' The digital policy literacy framework suggests that the myriad consumer complaints (as evidenced in the CRTC hearings) are a decisive entryway into increased mobilization around consumer and citizen concerns about the wireless infrastructure in Canada. A continued lack of competition and transparency is a key element of the public comments, and the CRTC is currently attempting to tackle this problem primarily through mandating that telecom providers increase the clarity of wireless contracts. The understanding of contracts can be seen as a tangible literacy component about the legal infrastructure that supports mobile communication, as discussed in the following section.

3. Infrastructures

Learning about the infrastructures that underpin mobile communication in Canada is crucial for shaping not just privacy policy activism, but the tactical decisions that young people make as consumers and users of mobile technologies. In our interviews and focus groups, we found that young people were already engaged in a number of privacy–protecting behaviors on their mobile devices, based on certain expectations around their informational privacy in networked spaces.

3.1. Control and consent in legal infrastructures

Even if our participants were ambivalent about mobile data collection, they still wished to exert control over how their information is collected and used. Particularly with information collected for the purposes of targeted advertising — on Facebook, Google, and other mobile apps — participants expressed a desire to understand and manage privacy settings. As Vicky said, she feels comfortable with data collection if it's something she has some control over, and if she expressly consents to it by using a particular app: 'if I choose it or if I download the app, then clearly I'm open to it.' Similarly, Stephanie asserted that 'if you're gonna download an app and you're going to be participating in that, I think you almost expect it now.' Using the service was seen as a kind of consent to information collection, evident in Wallis' summary of how she dealt with controlling privacy on social media apps:

> [...] especially in the way that Facebook changes so quickly, it's hard to keep up. And then you're like, oh wow, they changed the profile. And if you don't understand the way the new profile works, you can't really understand how to change your settings, so it's hard to adjust to these things quickly. But we, a couple times, have been doing Google searches of ourselves, and it's funny to see: I made all my tweets private, so that won't appear. And I don't have Facebook right now.

Wallis' choice to leave Facebook was partially motivated by the site's confusing privacy settings, which other participants also noted were frequently difficult to manage and often defaulted to the most public settings. As Stephanie said, 'I think you should be able to opt in to it,' rather than have to opt out.

3.2. Privacy policies as regulatory infrastructure

While using social media sites and apps was generally seen as a kind of consent for data collection, the participants felt that privacy policies should clearly outline exactly what kinds of personal information is collected and how it is used and/or shared with third parties. Consistent with research conducted by the Office of the Privacy Commissioner (OPC, 2009), these youth explained that privacy policies were not transparent enough for them to fully understand the extent of mobile data collection. As Charles noted, changes to privacy policies tended to coincide with defaults to new, privacy compromising features: 'So it's sketchy, 'cause it's one thing for you

to actively say you want to do that, but for them to just assume that they will roll out this new feature and you're going to use it whether you like it or not. That's on the sketchy side.' Our participants felt that the issue of literacy in privacy policies and terms of service was important; as Vicky said, she made herself aware of Facebook's terms so that 'it doesn't concern me as much as someone who's not aware of it.' Despite this claim for awareness, participants typically noted that they did not even read privacy policies, which reflects a prevalent trend described in existing research (Turow, *et al.*, 2008; boyd and Hargittai, 2010).

3.3. Commercial underpinnings of infrastructure: Location–based advertising

Literacy about privacy policies and terms of service is important because these documents are the manifestations of commercial contracts that dictate privacy rights for young people using these apps. The commercial infrastructure behind mobile data collection was especially apparent to our focus group participants through targeted ads, intrusive forms of advertising that often use location data to send promotional SMS messages or pop–up ads to mobile devices. As Nick described targeted mobile ads, 'I think that's partially a privacy issue but also just really annoying [...] because I feel like my texting on my phone is for two things, work — say if someone needs to reach me in an emergency — or my friends. That's it for me. I don't wanna get advertisements on my cell phone.' Ariel agreed that this kind of advertising was particularly intrusive: 'I feel like, especially text message, people get text messages from our friends, our family, it's personal. It's an intimate way of connecting with people and not to the rest of the marketing world.' Yet, if they could exert some control over location–based advertising, the participants reported that it would be less 'creepy'; as Vicky said: 'If at one point you could be like, I don't want any more information, if you could put a hold on it or stop it, that would be ok.'

The ability to control location–based ads was framed as a personal choice over whether to consent to targeted advertising more generally. Charles explained his personal boundary that would determine whether he was bothered by target marketers: 'As long as they don't get in my way, I'm not going to get in theirs, and they can just go about doing whatever they're doing.' These responses suggest that literacy about the infrastructures underpinning mobile privacy involves a recognition of how marketers target youth as consumers through mobile devices. While location–based advertising was sometimes experienced by this group of young people as surveillance, and was thus described by participants as troubling, most of the time ads were not intrusive enough to pose a real problem. The perception of control over targeted ads was also an important factor in how negatively ads might be perceived.

Conclusion

When illustrated by this group of young Canadians' discussions of mobile privacy, the digital policy literacy framework highlights how young people's mobile privacy is constructed as a consumer right. The participants in our study were all reasonably literate about mobile marketing practices, and understood that privacy was a tenuous right in mobile apps that are predicated on data collection. While they were concerned about their privacy in mobile and online environments, participants often felt ambivalent about privacy protection, given a lack of interest in making policy interventions and a feeling of mistrust toward wireless service providers. Moreover, the commercial infrastructures that govern privacy policies as legal contracts were framed in terms of surveillance and intrusion, but were often not explicitly threatening enough to take action against. Because this group of young Canadians expressed a fair degree of literacy about privacy settings, they felt that managing privacy on their mobiles was a matter of individual responsibility, and not necessarily a broader policy concern.

The trade–off that participants described between using the mobile service or app and relinquishing some personal privacy was framed as an everyday exchange governed by individual choice. Even if these young people claimed to understand the risks involved in having their data collected through mobile devices, they did acknowledge that not everyone shared their degree of literacy; as Nick said: 'I think most people are blinded by the convenience of whatever service or product they have without actually looking deeper and realizing, oh wait, there's all this other stuff that goes behind this that I wasn't aware of that's potentially going to bite me in the ass later.' Despite this contention that 'most people' were probably unaware of the consequences of information disclosure, none of the participants suggested that federal regulation was necessarily an appropriate course of action to address mobile privacy concerns.

We argue that these young people's reluctance to claim a role for policy interventions about mobile privacy, instead likening privacy protection to an individual responsibility, reflects a neoliberal trend in media policy more broadly that frames the citizen as consumer (Livingstone and Lunt, 2007; Thorson, 2012). In our focus group discussions and in federal regulatory discourse, citizen needs and the public good is replaced by consumer demands and fair business practices. The 2013 CRTC consultation on the wireless code was emblematic in this regard, in its 'development of a mandatory code for all mobile wireless service providers to address the clarity and content of wireless service contracts and related issues for consumers' (CRTC, 2013). Similarly, in our focus groups about mobile privacy, participants often described themselves as consumers making choices in a mobile marketplace based on issues of cost and convenience. The

lack of privacy in networked environments sometimes bothers these young people, but because it has not typically been experienced as a significant threat, they mostly feel ambivalent about mobilizing around privacy policy–making.

The role for the digital policy literacy framework in this context is to provide a rejoinder to the dominant consumer framing of privacy, in the form of a citizen–centric framing, whereby privacy is seen as a fundamental right in a democratic society. Given that privacy is shaped by current mobile and online marketing practices — and that government breaches of privacy also rest on commercial infrastructures of data collection, starkly illuminated by the recent revelations about the U.S. National Security Agency's Prism surveillance program's reliance on social media data (Greenwald and MacAskill, 2013; Rushe, 2013) — a citizen–focused framing lends a necessary policy imperative to delimit the power of commercial actors in determining how people's information gets collected and used. Literacy around not only why information privacy is important, but also how it might be guaranteed through policy measures, is the first step toward getting people to participate in policy–making. Such an intervention into digital literacy more broadly is especially crucial for young people growing up with digital and mobile technologies as ubiquitous communication infrastructure. For youth entering civic life through technology, literacy about digital policy issues will shape their lives as both consumers and citizens as they negotiate the constantly changing contours of participation.

About the authors

Leslie Regan Shade is Associate Professor in the Faculty of Information at the University of Toronto. Her research focus since the mid–1990s has been on the social and policy aspects of information and communication technologies (ICTs), with particular concerns toward issues of gender, youth and political economy.
E–mail: leslie [dot] shade [at] utoronto [dot] ca

Tamara Shepherd is a Postdoctoral Fellow at the Rogers School of Information Technology Management at Ryerson University. She has published on aspects of labour and literacy in digital culture and new media policy, from a feminist political economy perspective.
E–mail: tamara [dot] shepherd [at] ryerson [dot] ca

Acknowledgements

Notes

1. All participants consented to the use of their first names in any published material from this research.

2. Industry Canada, 2010, p. 30.

3. Industry Canada, 2010, p. 24.

4. Canadian Internet Registration Authority (CIRA), 2010, p. 4.

5. See OPC's Youth Privacy section at http://www.priv.gc.ca/youth-jeunes/index_e.asp and the OIPC privacy by design at http://www.privacybydesign.ca/.

6. O'Neill, 2010, p. 323.

7. Buckingham, 2010, p. 59.

8. Devitt and Roker, 2009, p. 194.

9. Shepherd, 2012, p. 102.

10. Office of the Privacy Commissioner (OPC), 2011, p. 12.

11. OPC, 2011, p. 28.

12. OPC, 2012, p. 2.

13. See for example: The FTC Staff Report (2013), available at http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm; the FTC report *Mobile Apps for Kids* (2012), available at http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf; and Pew's report *Privacy and Data Management on Mobile Devices* (2012), available at http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx.

14. See http://www.ftc.gov/opa/2013/02/path.shtm.

References

Donna E. Alvermann and Margaret C. Hagood, 2000. "Critical media literacy: Research, theory, and practice in 'New Times'," *Journal of Education Research*, volume 93, number 3, pp. 193–205. http://dx.doi.org/10.1080/00220670009598707, accessed 16 September 2013.

Darin Barney, 2005. *Communication technology*. Vancouver: UBC Press.

David Bawden, 2001. "Information and digital literacies: A review of concepts," *Journal of Documentation*, volume 57, number 2, pp. 218–259. http://dx.doi.org/10.1108/EUM0000000007083, accessed 16 September 2013.

Aaron Beach, Mike Gartrell and Richard Han, 2009. "Solutions to security and privacy issues in mobile social networking," *CSE '09: Proceedings of the 2009 International Conference on Computational Science and Engineering*, volume 4, pp. 1,036–1,042. http://dx.doi.org/10.1109/CSE.2009.243, accessed 16 September 2013.

Shirley J. Behrens, 1994. "A conceptual analysis and historical overview of information literacy," *College and Research Libraries*, volume 55, number 4, pp. 309–322.

Geoffrey C. Bowker, Karen Baker, Florence Millerand and David Ribes, 2010. "Towards information infrastructure studies: Ways of knowing in a networked environment," In: Jeremy Hunsinger, Lisbeth Klastrup and Matthew Allen (editors). *International handbook of Internet research*. Berlin: Springer–Verlag, pp. 97–117. http://dx.doi.org/10.1007/978-1-4020-9789-8_5, accessed 16 September 2013.

danah boyd and Eszter Hargittai, 2010. "Facebook privacy settings: who cares?" *First Monday*, volume 15, number 8, at http://firstmonday.org/article/view/3086/2589, accessed 12 March 2013.

danah boyd, Jenny Ryan and Alex Leavitt, 2011. "Pro–self–harm and the visibility of youth–generated problematic content," *I/S: A Journal of Law and Policy for the Information Society*, volume 7, number 1, pp. 1–32.

David Buckingham, 2010. "Defining digital literacy: What young people need to know about digital media," In: Ben Bachmair (editor). *Medienbildung in neuen Kulturräumen: Die deutschprachige und britische Diskussion*. Berlin: VS Verlag für Sozialwissenschaften, pp. 59–71. http://dx.doi.org/10.1007/978-3-531-92133-4_4, accessed 16 September 2013.

Canadian Internet Registration Authority (CIRA), 2010. *Submission to the Digital Economy Strategy Consultation* (14 July), at http://www.ic.gc.ca/eic/site/028.nsf/eng/00256.html, accessed 10 January 2013.

Canadian Radio–television and Telecommunications Commission (CRTC), 2013. "Telecom Notice of Consultation 2012–557–1. Proceeding to establish a mandatory code for mobile wireless services," at http://www.crtc.gc.ca/eng/archive/2012/2012-557-1.htm, accessed 11 March 2013.

Maurice Charland, 1986. "Technological nationalism," *Canadian Journal of Political and Social Theory/Revue canadienne de théorie politique et sociale*, volume 10, numbers 1–2, pp. 196–220.

Lynn Schofield Clark, 2013. *The parent app: Understanding families in the digital age*. New York: Oxford University Press.

Giuliana Cucinelli and Leslie Regan Shade, 2012. *Our privacy matters! Youth, identity and online sociability* [video], at http://ourprivacymatters.ca, accessed 23 June 2013.

Kerry Devitt and Debi Roker, 2009. "The role of mobile phones in family communication," *Children & Society*, volume 23, number 3, pp. 189–202. http://dx.doi.org/10.1111/j.1099-0860.2008.00166.x, accessed 16 September 2013.

Nora R.A. Draper, 2011. "Is your teen at risk? Discourses of adolescent sexting in United States television news," *Journal of Children and Media*, volume 6, number 2, pp. 221–236. http://dx.doi.org/10.1080/17482798.2011.587147, accessed 16 September 2013.

Maeve Duggan and Lee Rainie, 2012. "Cell phone activities 2012" (25 November), *Pew Internet & American Life Project*, at http://pewinternet.org/Reports/2012/Cell-Activities/Main-Findings.aspx, accessed 16 September 2013.

David Finkelhor, 2010. "The Internet, youth deviance and the problem of juvenoia" [video] (22 October), at http://vimeo.com/16900027, accessed 10 January 2013.

Des Freedman, 2008. *The politics of media policy*. Cambridge: Polity Press.

Hernan Galperin, 2004. "Beyond interests, ideas, and technology: An institutional approach to

communication and information policy," *Information Society*, volume 20, number 3, pp. 159–168. http://dx.doi.org/10.1080/01972240490456818, accessed 16 September 2013.

Tarleton Gillespie, 2007. *Wired shut: Copyright and the shape of digital culture*. Cambridge, Mass.: MIT Press.

Gerard Goggin, 2013. "Youth culture and mobiles," *Mobile Media & Communication*, volume 1, number 1, pp. 83–88.

Glen Greenwald and Ewen MacAskill, 2013. "NSA Prism program taps in to user data of Apple, Google, and others," *Guardian* (6 June), at http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, accessed 28 August 2013.

Stuart Hamilton and Niels Ole Pors, 2003. "Freedom of access to information and freedom of expression: The Internet as a tool for global social inclusion," *Library Management*, volume 24, numbers 8–9, pp. 407–416. http://dx.doi.org/10.1108/01435120310501086, accessed 16 September 2013.

Renee Hobbs, 2011. *Digital and media literacy: Connecting culture and classroom*. London: Corwin Press.

Michael Hoechsmann and Stuart R. Poyntz, 2012. *Media literacies: A critical introduction*. Malden, Mass.: Wiley–Blackwell.

Industry Canada, 2010. *Improving Canada's digital advantage: Strategies for sustainable prosperity. Consultation paper on a Digital Economy Strategy for Canada*. Ottawa: Government of Canada, at http://publications.gc.ca/collections/collection_2010/ic/Iu4-144-2010-eng.pdf, accessed 16 September 2013.

Robert Jeffery, 2008. "Mobile forms of communication and the transformation of relations between the public and private spheres," In: Karen Ross and Stuart Price (editors). *Popular media and communication: Essays on publics, practices and processes*. Newcastle: Cambridge Scholars Publishing, pp. 5–23.

Bobbie Johnson, 2010. "Privacy no longer a social norm, says Facebook founder," *Guardian* (10 January), at http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy, accessed 22 December 2012.

Douglas Kellner and Jeff Share, 2007. "Critical media literacy: Crucial policy choices for a twenty–first–century democracy," *Policy Futures in Education*, volume 5, number 1, pp. 59–69. http://dx.doi.org/10.2304/pfie.2007.5.1.59, accessed 16 September 2013.

John Lawford, 2008. *All in the data family: Children's privacy online*. Ottawa: Public Interest Advocacy Centre (PIAC), at http://www.piac.ca/files/children_final_small_fixed.pdf, accessed 16 September 2013.

Amanda Lenhart, 2012. "Teens, smartphones & texting" (19 March), *Pew Internet & American Life Project*, at http://www.pewinternet.org/~/media/Files/Reports/2012/PIP_Teens_Smartphones_and_Texting.pdf, accessed 16 September 2013.

Sonia Livingstone, 2008. "Engaging with media — a matter of literacy?" *Communication, Culture & Critique*, volume 1, number 1, pp. 51–62. http://dx.doi.org/10.1111/j.1753-9137.2007.00006.x, accessed 16 September 2013.

Sonia Livingstone and David R. Brake, 2010. "On the rapid rise of social networking sites: New findings and policy implications," *Children & Society*, volume 24, number 1, pp. 75–83. http://dx.doi.org/10.1111/j.1099-0860.2009.00243.x, accessed 16 September 2013.

Sonia Livingstone and Peter Lunt, 2007. "Representing citizens and consumers in media and communications regulation," *Annals of the American Academy of Political and Social Science*, volume 611, number 1, pp. 51–65. http://dx.doi.org/10.1177/0002716206298710, accessed 16 September 2013.

Graham Longford, 2011. "Spectrum policy: Squandering the digital dividend?" In: Marita Moll and Leslie Regan Shade (editors). *The Internet tree: The state of telecom policy in Canada 3.0*. Ottawa: Canadian Centre for Policy Alternatives, pp. 123–135, and at http://www.policyalternatives.ca/publications/reports/internet-tree, accessed 16 September 2013.

Clara Mancini, Keerthi Thomas, Yvonne Rogers, Blaine A. Price, Lukazs Jedrzejczyk, Arosha K. Bandara, Adam N. Joinson and Bashar Nuseibeh, 2009. "From spaces to places: Emerging contexts in mobile privacy," *Ubicomp '09: Proceedings of the 11th International Conference on Ubiquitous Computing*, pp. 1–10. http://dx.doi.org/10.1145/1620545.1620547, accessed 16 September 2013.

Alice E. Marwick, Diego Murgia–Diaz and John Palfrey, 2010. "Youth, privacy and reputation: Literature review," *Berkman Center Research Publication*, number 2010–5; *Harvard Public Law*

Working Paper, number 10–29, at http://ssrn.com/abstract=1588163, accessed 11 December 2012.

Gary T. Marx and Valerie Steeves, 2010. "From the beginning: Children as subjects and agents of surveillance," *Surveillance & Society*, volume 7, numbers 3–4, pp. 192–230, and at http://www.surveillance-and-society.org/ojs/index.php/journal/article/view/beginning/beginning, accessed 16 September 2013.

Robert McChesney, 2013. *Digital disconnect: How capitalism is turning the Internet against democracy*. New York: New Press.

Media Awareness Network, 2010. "Digital literacy in Canada from inclusion to transformation," at http://www.ic.gc.ca/eic/site/028.nsf/eng/00454.html, accessed 10 December 2012.

MediaSmarts, 2012. "Young Canadians in a wired world, phase III: Talking to parents and youth about life online," at http://mediasmarts.ca/research-policy, accessed 29 December 2012.

Vincent Mosco, 2009. *The political economy of communication*. Second edition. Thousand Oaks, Calif.: Sage.

Philip M. Napoli and Minna Aslama (editors), 2010. *Communication research in action: Scholar–activist collaborations for a democratic public sphere*. New York: Fordham University Press.

Christena Nippert–Eng, 2010. *Islands of privacy*. Chicago: University of Chicago Press.

Peter Nowak, 2010. "Canadian wireless firms still tops in profit: report," *CBC News* (19 July), at http://www.cbc.ca/technology/story/2010/07/19/canada-wireless-profit.html, accessed 22 October 2012.

Office of the Privacy Commissioner of Canada (OPC), 2013. "Announcement: Privacy Commissioner launches privacy mobile application" (28 January), at http://www.priv.gc.ca/media/nr-c/2013/an_130128_e.asp, accessed 15 March 2013.

OPC, 2012. "Seizing opportunity: Good privacy practices for developing mobile apps," at http://www.priv.gc.ca/information/pub/gd_app_201210_e.asp, accessed 16 September 2013.

OPC, 2011. "Report on the 2010 Office of the Privacy Commissioner of Canada's consultations on online tracking, profiling and targeting and cloud computing," at https://www.priv.gc.ca/resource/consultations/report_201105_e.asp, accessed 16 September 2013.

OPC, 2009. "Social network site privacy: A comparative analysis of six sites," at https://www.priv.gc.ca/information/research-recherche/2009/sub_comp_200901_e.asp, accessed 16 September 2013.

Organisation for Economic Co–operation and Development (OECD), 2011. "OECD communications outlook 2011," at http://www.oecd.org/sti/broadband/oecdcommunicationsoutlook2011.htm, accessed 16 September 2013.

Brian O'Neill, 2010. "Media literacy and communication rights: Ethical individualism in the new media environment," *International Communication Gazette*, volume 72, numbers 4–5, pp. 323–338.
http://dx.doi.org/10.1177/1748048510362445, accessed 16 September 2013.

Brian O'Neill and Ingun Hagen, 2009. "Media literacy," In: Sonia Livingstone and Leslie Haddon (editors). *Kids online: Opportunities and risks for children*. Bristol: Polity Press, pp. 229–239.

John Palfrey, Urs Gasser, Miriam Simun and Rosalie Fay Barnes, 2009. "Youth, creativity, and copyright in the digital age," *International Journal of Learning and Media*, volume 1, number 2, pp. 79–97.
http://dx.doi.org/10.1162/ijlm.2009.0022, accessed 16 September 2013.

Sora Park, 2012. "Dimensions of digital media literacy and the relationship with social exclusion," *Media International Australia*, number 142, pp. 87–100.

Quorus, 2012. "Cell phone consumer attitudes study" (23 April), at http://cwta.ca/wordpress/wp-content/uploads/2011/08/CWTA-2012ConsumerAttitudes1.pdf, accessed 22 December 2012.

Kate Raynes–Goldie, 2010. "Aliases, creeping and wall cleaning: Understanding privacy in the age of Facebook," *First Monday*, volume 15, number 1, at http://firstmonday.org/article/view/2775/2432, accessed 20 December 2012.

Dominic Rushe, 2013. "Facebook reveals government asked for data on 38,000 users in 2013," *Guardian* (28 August), at http://www.theguardian.com/technology/2013/aug/27/facebook-government-user-requests, accessed 28 August 2013.

Leslie Regan Shade, 2012. "Toward a model of digital policy literacy," *iConference '12: Proceedings of the 2012 iConference*, pp. 459–461.

http://dx.doi.org/10.1145/2132176.2132247, accessed 16 September 2013.

Tamara Shepherd, 2012. "Persona rights for user–generated content: A normative framework for privacy and intellectual property regulation," *tripleC: Communication, Capitalism & Critique*, volume 10, number 1, pp. 100–113, and at http://www.triple-c.at/index.php/tripleC/article/view/305, accessed 16 September 2013.

Tamara Shepherd and Leslie Regan Shade, 2012. "Mobile phones as a 'necessary evil': Canadian youth talk about their mobile phones," In: Phillip Vannini, Lucy Budd, Christian Fisker, Paola Jirón and Ole B. Jensen, (editors). *Technologies of mobility in the Americas*. New York: Peter Lang, pp. 199–213.

Katie Shilton, 2009. "Four billion little brothers? Privacy, mobile phones, and ubiquitous data collection," *Communications of the ACM*, volume 52, number 11, pp. 48–53. http://dx.doi.org/10.1145/1592761.1592778, accessed 16 September 2013.

Gitte Stald, 2007. "Mobile identity: Youth, identity, and mobile communication media," In: David Buckingham (editor). *Youth, identity, and digital media*. Cambridge, Mass.: MIT Press, pp. 143–164, and at http://digimed-jhi.pbworks.com/f/Stald%2BMobile%2BIdentity.pdf, accessed 16 September 2013.

Valerie Steeves and Cheryl Webster, 2008. "Closing the barn door: The effect of parental supervision on Canadian children's online privacy," *Bulletin of Science, Technology & Society*, volume 2, number 1, pp. 4–19. http://dx.doi.org/10.1177/0270467607311488, accessed 16 September 2013.

Kjerstin Thorson, 2012. "What does it mean to be a good citizen? Citizenship vocabularies as resources for action," *Annals of the American Academy of Political and Social Science*, volume 644, number 1, pp. 70–85. http://dx.doi.org/10.1177/0002716212453264, accessed 16 September 2013.

Bernie Trilling and Charles Fadel, 2009. *21st century skills: Learning for life in our times*. San Francisco: Jossey–Bass.

Sherry Turkle, 2011. *Alone together: Why we expect more from technology and less from each other*. New York: Basic Books.

Kathleen Tyner, 1998. *Literacy in a digital world: Teaching and learning in an age of information*. Mahwah, N.J.: Erlbaum.

Jennifer M. Urban, Chris Jay Hoofnagle and Su Li, 2012. "Mobile phones and privacy," *UC Berkeley Public Law Research Paper*, number 2103405, at http://ssrn.com/abstract=2103405, accessed 13 January 2013.

Martha J. Whitehead and Catherine A. Quinlan, 2002. *Canada: An information literacy case study*. White paper prepared for UNESCO, U.S. National Commission on Libraries and Information Science and National Forum on Information Literacy.

Editorial history