30
Digital Privacy Policy Literacy: *A Framework for Canadian Youth*

Leslie Regan Shade and Sharly Chan

Introduction

This chapter focuses on digital privacy policy literacy for youth in the Canadian context by anchoring its discussion in the findings of a study conducted by MediaSmarts and the eQuality Project about young people's decision-making around photo sharing and privacy on social media. Building on tenets of media and information literacy (MIL), digital privacy policy literacy expands on a framework for digital policy literacy that comprises three elements: policy processes, political economy, and infrastructures. This chapter will first describe the model of digital policy literacy within the MIL paradigm. Then, a brief overview of the study on photo-sharing applications and privacy will be explicated using the three elements of the digital policy literacy model, highlighting keywords that form each element. Keywords derive from an intellectual trajectory in communication, media, and cultural studies, where they are used to interrogate problems, advance theory, and organize teaching. From Raymond Williams' (1976) seminal work, *Keywords*, to more recent volumes on *Digital Keywords* (Peters 2016) and *Keywords for Media Studies* (Ouellette and Gray 2017), keywords serve as a pedagogical tool to delimit and define crucial terminology in scholarly fields. As part of a larger research project on young adults and digital privacy, keywords allow us to investigate the nuances and contours of digital privacy policy literacies and shed light on these issues beyond the Canadian context.

Digital Policy Literacy

Digital policy literacy is aligned with critical approaches to MIL encompassing a global framework comprising three elements: (i) an understanding of digital policy processes, (ii) the political economy of digital media, and (iii) technological infrastructures.

The first element, *policy processes*, is concerned with the governance of communication resources at local, national, and global levels; how policy issues are created and get on the agenda; and structures of participation in policy processes, including various institutions of policy governance, informal and formal mechanisms for public participation, and the role of stakeholders in policy contexts.

The second, *political economy,* is concerned with the broader social, economic, and political relations surrounding the ownership, production, and distribution of digital and communication resources by media industries and institutions, as well as their consumption and creation by users.

Third, *infrastructures* are socio-technical systems consisting of diverse technical infrastructures of operating systems and related applications and features such as location-based devices, as well as knowledge infrastructures governed by standards, operating procedures, and international governance regimes. For each element of the digital policy literacy model, a series of questions can be broached, as Table 30.1 illustrates.

Prior research has used the model of digital policy literacy to examine young people's engagement with digital and mobile technologies. One study about young people's conception of privacy on their mobile phones and apps highlighted how their mobile privacy is constructed as a consumer right. While the participants were fairly cognizant about mobile marketing practices and understood that privacy was a tenuous right in mobile apps predicated on data collection, they felt ambivalent about privacy protection and expressed a palpable mistrust toward wireless service providers (Shade and Shepherd 2013).

In another study, the digital policy literacy model was used to examine young women's knowledge of telecommunication infrastructure through their YouTube activism against usage-based billing (UBB): a practice allowing internet service providers (ISPs) to calculate how much data their users upload to or download from the internet and charge them according to their data usage. The model highlights how the young women displayed an awareness of policy stakeholders, telecommunications ownership, and infrastructural constraints in the UBB debate (Shade 2015).

The model was also used to support the development of digital policy literacy for a project funded by the Office of the Privacy Commissioner Contributions Program, "Co-Designing Open Badges for Privacy Education with Canadian Youth." This was a Toronto-based co-design project involving eight teenagers and the global nonprofit organization Mozilla (Smith et al. 2015). The project goals were to empower young people to create prototype-level open badges and teaching activities in the form of open educational resources (OERs) relevant to digital privacy in the Canadian context (Smith et al. 2017).

Table 30.1 A global model of digital policy literacy.

Policy processes	How is policy constituted? What are the structures of participation in policy-making? What are effective modes of activism and intervention to shape policy?
Political economy	What are the socio-political relations surrounding the ownership, production, distribution, and consumption of digital media? How do they reinforce, challenge, or influence social relations of class, gender, and race?
Infrastructures	How do technological affordances and design activate or inhibit online interactions? What is their impact on ownership of content, privacy protection, access, and communication?

To Share or Not to Share

A study of how young people make decisions about the privacy of the photos they share on social media platforms was conducted in late 2016 by MediaSmarts, a Canadian digital literacy organization, and the eQuality Project, a Canadian research partnership of scholars, policymakers, educators, community organizations, and youth with a mandate to inform digital economy policies through the creation of new knowledge about how diverse groups of young people conceptualize privacy and the potential for equality in networked spaces.

Funded by the Office of the Privacy Commissioner of Canada through its Contributions Program, the study, *Decision-Making and Privacy: How Youth Make Choices About Reputational Data and Privacy Online*, engaged 18 diverse young people between the ages of 13 and 16 living in Ottawa to keep a diary of photos they shared with others online over one week. Participants were asked to categorize the photos they were comfortable sharing with lots of people or a few people, and to select a photo they did not wish to share with anyone (which they could describe in writing). This was followed by an interview between the researchers and the participant. Participants first discussed their practices and preferences related to photo sharing in general and then explicated their decision-making process about the types of personal information they would willingly disclose online, their strategies for reputation and privacy management, and their knowledge of fair information practices toward their personal information (Johnson et al. 2017).

The next sections of the chapter use the findings of the study to outline the utility of the digital privacy policy literacy framework. The analysis starts with the political economy, and then continues to infrastructures, and finally, policy processes. Keywords for each element of the framework, listed in separate tables and further italicized and described within each section, derive from the findings of the study and reflect data privacy concepts, mechanisms, and governance.

Political Economy

Social media companies are powerful and popular entities that increasingly shape the everyday communicative practices of young people (see Table 30.2). Photo-sharing applications such as Instagram and Snapchat are among the top social media applications that North American teens use. Findings from a 2018 Pew Research Center study revealed that 72% of American teens use Instagram, 69% use Snapchat, and 59% use Facebook (Anderson and Jiang 2018). A 2017 survey from RBC Capital Markets detailed that the "teen cohort" demographic, ages 13–18, prioritized the use of Snapchat (79%), Instagram (73%), Facebook (57%), and Twitter (39%) (RBC Capital Markets 2017).

Table 30.2 Political economy keywords for photo-sharing applications.

Political economy	Antitrust Attention Attention economy Competition Data sharing Market power Ownership of Instagram and Snapchat

Instagram, created in 2010, is one of the most used photo-sharing applications for youth, and "within two years, the app had 30 million users. It would grow to 70 million users by the end of 2012" (Wu 2018). As a result of its growth rate and penchant for attracting a younger demographic, Instagram was a competitor to social media platforms such as Facebook, who thus acquired it in 2012 for US$1 billion (Rusli 2012).

Snapchat, a photo-sharing and messaging app, attracted a user group comprising high school students and young adults because of its feature of ephemerality that let people send messages that would disappear within seconds. In 2013, the company Snap reportedly turned down a US$3 billion acquisition offer from Facebook (Wall Street Journal 2013). Its 2017 initial public offering (IPO: the issuing of public shares to allow companies to raise capital from public investors) filing to the Securities and Exchange Commission (SEC), six years after its creation, detailed that 158 million people use Snapchat on average daily, with over 2.5 billion snaps created every day (Snap Inc. 2017).

A key issue from Facebook's acquisition of Instagram relates to *competition* and *antitrust* law. Tim Wu, a professor at Columbia University, states how antitrust agencies usually intervene when a company wants to acquire a competitor, but "in the case of Facebook and Instagram, the agencies confronted two firms that did not charge users, instead competing chiefly for time and *attention*. As Instagram hadn't begun to sell ads, the antitrust agencies were unable to see a problem" (Wu 2018). This allowed Facebook to monopolize the social media platform space, as it no longer had to compete for users. Soon after the acquisition, Instagram announced that it would display ads to its US-based users (Panzarino 2013).

Facebook has consolidated its *market power,* according to Wu, "by piling on more ads for users, jacking up its advertising rates and also invading privacy without fear of people fleeing for an attractive rival – even if it remains 'free'" (Wu 2018). The business model of social media is dependent on the *attention economy*, wherein the stickiness of eyeballs to relatable advertising and clickable and "likeable" features feeds on a push for user popularity (van Dijck 2013, p. 62).

The MediaSmarts/eQuality Project photo-sharing study found that "almost none of the participants had a clear idea of what the corporations that owned the platforms they use did with their photos or, indeed, showed an awareness of these platforms as corporate spaces at all" (Johnson et al. 2017, p. 4). Facebook's *ownership* of Instagram is not made clear to users as they exist as separate platforms that appear to be competing. *Data sharing* is enabled by these two platforms, specifically to target ads and to grow the network by suggesting friends from existing lists from Facebook to Instagram or vice versa (Instagram 2019a, b). These competition and antitrust issues are even more concerning with Facebook's earlier attempt to acquire Snap.

Wu has suggested reversing the merger between Facebook and Instagram, since the US government may undo it if it "violates the law, especially when there is reason to suspect regulators didn't understand the markets well enough at the time of the actual merger" (Wu 2018). In this case, traditional notions of competition that revolve around price are not sufficient for the "free" platform economy where the metric lies with views and usage.

Infrastructures

The digital infrastructure of photo-sharing apps shapes how users interact with a platform (see Table 30.3). Its design can influence user behavior and change how users understand consent and privacy. Findings from the MediaSmarts/eQuality Project study reveal how teens' "concerns about privacy, reputation and consent are nearly all focused on managing how they are seen by 'people' online" (Johnson et al. 2017, p. 4). Notions of privacy are tied to *social capital* and its management through different platforms. Teens see Instagram as a more curated and refined space than Snapchat, which uses temporary photos. *Privacy management* is illustrated by teens who "are not only choosing different platforms to manage their privacy and publicity: they are also, consciously or not, being influenced by the structure of those platforms" (Johnson et al. 2017, p. 3). This means that privacy is mediated through context: "they expect Snapchat not to save any of their photos, since in their minds they've sent a clear signal that the photos should be temporary by choosing that platform" (Johnson et al. 2017, p. 4). If the platform discourages their friends from saving their temporary photos with screenshot notifications, they expect that the platform will not save them.

The study noted a few strategies that teens use to manage their social capital online, to include bridging and bonding relationships (identity development; building trust among peers; mediating relationships; connecting to broader social networks, online and offline). For instance, photos must "be personal, but not revealing." This means that these privacy strategies may have "restricted the potential of social media to support free expression" (Johnson et al. 2017, p. 2). Management of social capital with peers takes a more context-based approach as they "expected their peers to ask before posting a photo of them" and expected that photos shared on platforms like Snapchat would not be shared, following the functionality of the digital infrastructure that only encourages temporary photos (Johnson et al. 2017, p. 3). These tactics are context-sensitive and change fluidly at any point in time with the retroactive consent of photos. They correspond to MIL competencies of critical thinking and consumer awareness, including management of self-image and self-reputation.

Table 30.3 Infrastructure keywords for photo-sharing applications.

Infrastructures	Consent Default settings Privacy management Privacy policies Social capital Terms of service

While some of these privacy tactics can manage reputation and reduce misuse of personal information, they do not work for the data structures that underlie the platform. The current regulatory framework requires users to agree to all of the *terms of service* before using the platform, differing greatly from the context-based model of consent that teens may expect from these platforms. However, people often accept these terms of service agreements and *privacy policies* without reading them because they are lengthy and difficult to understand (Johnson et al. 2017. p. 4; OPC 2018d).

Since Facebook's acquisition of Instagram, its digital infrastructure has changed from the addition of data-sharing agreements between the two companies to new features such as the activity statuses of users on the platform (Instagram 2019c, d). The platform has added privacy-enhancing features to provide more privacy options to users, such as a "close friends" option to share Instagram stories with a select group of people (Instagram 2019e). However, these privacy features and settings are often unknown by the larger public, let alone young

people. As a result, *default settings* are extremely important because new users "are the least likely to adjust how their account is set up regarding privacy matters" (Boyd and Hargittai 2010). Users need to opt in or change default settings to have better privacy and security on their social media accounts.

Even if users are MIL-diligent and have developed their safety competencies and put in the necessary labor to change these settings, the digital infrastructure can affect privacy assumptions and settings. In May 2018, a software bug on Facebook affected 14 million users when it "updated the audience for some users' posts to 'public' without any warning" (Wagner 2018). In addition to this type of data and information breach, new updates can be confusing and frustrating with features that cannot be turned off, or settings that are invisible to the user. For example, Instagram's display feature shows whether you or your friends liked a photo with text under the photo that says "@username and 10,000 others liked this" (Instagram 2019b). It may chill freedom of expression if a user does not want others to see that they liked something. These new features can challenge *consent* (when users can meaningfully agree to and understand how their personal information is collected, used, and disclosed by organizations) or change the ways people interact with the platform.

Policy Processes

It can be difficult to navigate privacy, consent, and terms of service on photo-sharing applications (see Table 30.4). In Canada, privacy regulatory bodies and legislation help protect users' privacy. However, these organizations are often limited in their capacity to address concerns due to the lack of legislative tools, educational resources, or enforcement mechanisms. There is a recognized need to update legislation to account for technological developments, user experiences, and heightened corporate data breaches.

Table 30.4 Policy process keywords for photo-sharing applications.

Policy processes	Civil society groups Enforcement powers General Data Protection Regulation (GDPR) Meaningful consent Office of the Privacy Commissioner of Canada (OPC) Personal information Personal Information Protection and Electronic Documents Act (PIPEDA) Privacy Act

The Office of the Privacy Commissioner of Canada (OPC) is an oversight and regulatory body that oversees compliance of federal privacy legislation and protects and promotes privacy rights. It is responsible for *the Privacy Act* (federal legislation that regulates data collection, use, disclosure, and disposal of personal information held by the federal government and federal agencies) and the *Personal Information Protection and Electronic Documents Act* – PIPEDA (federal legislation that regulates information-handling practices for private companies across Canada) (OPC 2018b). The OPC also conducts, funds, and publishes research into privacy issues, reports on personal information–handling practices, and promotes public awareness and understanding of privacy issues (OPC 2018a). It creates and makes resources available on privacy for teachers, parents, businesses, and children.

Its recent work includes a consultation to update PIPEDA (OPC 2018c), which protects individuals by allowing or prohibiting "organizations to collect, use and disclose personal information, depending on their purposes for doing so" (OPC 2018d). Under PIPEDA, *personal information* "includes any factual or subjective information, recorded or not, about an identifiable individual" such as "age, name, ID numbers, income … opinions, evaluations, comments" (OPC 2018e). In addition, IP (internet protocol) and MAC (computer hardware) addresses are also considered to be personal information "if it can be associated with an identifiable individual" (OPC 2013).

One of the outcomes of the consultation was OPC's guidance document that examined how to obtain *meaningful consent*. As it described this concept, under PIPEDA, individuals need to

"understand the nature, purpose, and consequences of what they are consenting to. In order for consent to be considered valid or meaningful, organizations must inform individuals of their privacy practices in a comprehensive and understandable manner" (OPC 2018d). This document provides guiding principles to obtain meaningful consent such as "emphasizing certain key elements in privacy information and explaining them in a user friendly way, providing people with clear options to say 'yes' or 'no', and making consent a dynamic and ongoing process" (OPC 2018d). In addition, the OPC identified situations of inappropriate uses of data and "no-go zones," which outline what data organizations are prohibited from collecting. These guidelines follow a more realistic understanding of consent and privacy expectations in the digital age. The OPC's ongoing investigations, reports, and research into privacy matters position the OPC to be a key component of the policy process and privacy advocacy in Canada.

The European Union has transformed its personal data and privacy protection regulation with the *General Data Protection Regulation (*GDPR), implemented on 25 May 2018. Key changes under GDPR include the increase of territorial scope to apply to all companies that process the personal data of all data subjects that reside in the EU, regardless of where the company is located (GDPR art. 3.1). Conditions for consent are stronger, requiring companies to present written agreements "in an intelligible and easily accessible form, using clear and plain language. The data subject shall have the right to withdraw his or her consent at any time. It shall be as easy to withdraw as to give consent" (GDPR art. 7.1, 7.3). The new guidelines on consent for PIPEDA are similar to the consent provisions in the GDPR that provide more protection in the digital age. The GDPR also recognizes that "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data" and details specific provisions related to the use of children's personal data for marketing and data collection (General Data Protection Regulation 2016).

One of the major legislative issues with the privacy framework in Canada is the lack of *enforcement mechanisms* for the OPC and other provincial regulators. Currently, the OPC can investigate privacy complaints and enforce privacy violations through public interest disclosure/naming, compliance agreements, reporting offenses to the Auditor General, auditing, and presenting the violation to the federal court (OPC 2017b). In the OPC's 2016–2017 Annual Report to Parliament, it noted how its consultations on PIPEDA with *civil society groups* strongly suggested greater enforcement powers, "arguing that self-regulation currently does not work" (OPC 2017a, p. 16). It further noted that "consumers clearly expect stronger enforcement in all forms, including orders, fines and audits" (OPC 2017a, p. 16).

The need for stronger and more effective enforcement mechanisms was reiterated in the OPC's 2017–2018 Annual Report. Reflecting on revelations of the mining of users' Facebook data by the UK data analytics firm Cambridge Analytica and other corporate data breaches, OPC Privacy Commissioner Daniel Therrien starkly states, "the time of self-regulation is over" (OPC 2018f, p. 8). Indeed, the House of Commons Standing Committee on Access to Information, Privacy and Ethics released a report four months after the Annual Report on the breach of personal information by Cambridge Analytica and Facebook, recommending several amendments to PIPEDA, including giving enforcement powers to the privacy commissioner with respect to fines for noncompliance and the power both to require organizations to produce relevant documents in a timely fashion and to seize documents during an investigation (House of Commons, Canada 2018).

Four months after the House of Commons report, the OPC and the BC Information and Privacy Commission (OIPC) released findings from their year-long report on Facebook and Cambridge Analytica. They determined that Facebook had violated federal and BC provincial privacy statutes and further announced the filing in federal court of a legal suit against Facebook seeking an order to implement their joint recommendations to Facebook, including one that requires obtaining meaningful consent from its users (Tunney 2019). In the GDPR, enforcement of the regulation is done through tiered fines with a maximum of 4% of the total worldwide annual turnover or 20 million EUR (whichever is higher) (GDPR, art. 83.5).

Stronger enforcement mechanisms in the Canadian context, such as those sought by the OPC and OIPC, may help regulators protect and enforce privacy and data protection.

For the participants in the MediaSmarts/eQuality Project study, concerns surrounding privacy, reputation, and consent focused on their online visibility by friends, peers, family, and future audiences. They did not reflect on the corporate power of the platforms and the business model reliant on advertising. Understanding the legal implications of terms of service and consent is also complicated for these teens, as "they imagine a model of consent that is much closer to that which they expect from their peers" (for instance, expecting peers to ask their permission before posting a photo of them) and one "sensitive to context, as it is in relation to peers" (Johnson et al. 2017. p. 37). In addition, few of the teens read or, if they did, understood the nuances of the privacy policies and terms of service: "the participants generally felt that they were unable to give *meaningful* consent because the documents were too long and difficult to read" (Johnson et al. 2017, p. 37, emphasis in original). Given their feelings of disempowerment about negotiating their terms of engagement with the platforms, the participants did not express a right to privacy, and they were unaware of privacy legislation such as PIPEDA or fair information principles.

Conclusions

For young people, the nuances of digital privacy can be distinguished through their varying contexts. The MediaSmarts/eQuality Project study corroborates the privacy distinctions made by Livingstone et al. (2018, pp. 13–16) for capturing the dynamics of youth privacy: (i) interpersonal privacy (focus on the social environment, sharing practices, self-expression, participation, and social capital); (ii) institutional privacy (data collection by governments, schools, and other aligned third party organizations); and (iii) commercial privacy (datafication by corporate platforms and apps reliant on behavioral marketing and data-mining algorithms to collect and transmit personal information, which complicates the protection and autonomy of personal information).

In the photo-sharing study, teens were primarily concerned with their interpersonal privacy, to connect with friends, document shared memories, and seek peer approval. They did not perceive the photo-sharing platforms as "corporate *entities*" (Johnson et al. 2017, p. 4, emphasis in original) but rather as tools with which to manage and facilitate their online image and social interactions. Their concerns around privacy, consent, and reputation were thus suffused in their own curatorial role and how people (friends, family, or future audiences) saw them online. Their knowledge of commercial privacy was weak, and as the report argued, effective privacy education must thus "begin with not just digital literacy but key principles of *media* literacy, as youth are unaware both of the commercial considerations of the platforms they use and the way in which those considerations, and the technical considerations of those platforms, influence how and how much they share" (Johnson et al. 2017, p. 35, emphasis in original).

The digital privacy policy literacy model is therefore a useful framework for educators and students to adopt in order to examine the different components of digital privacy within the larger framework and principles of MIL that advocate, inter alia, critical thinking, consumer awareness, and online safety competencies and strategies. Applied to the photo-sharing study, the following aspects for each element can be discerned and added as a contribution to media education at large:

- *Policy processes*: Provides youth with an understanding of how privacy policy is created and enforced: for example, through diverse governance bodies like privacy and data commissions. Becoming familiar with privacy legislation – at the national and global level, and the privacy policies and terms of service on social media platforms and apps – develops in youth a consciousness of how they are implicated as consumers, and how they can participate in policy-making processes as engaged citizens to formulate their right to privacy.

- *Political economy of media systems and digital platforms and apps*: Allows youth to understand the ownership of the commercial sites and applications they use. In particular, it allows youth to develop an awareness of the market power and business model of social media, and how social and mobile media are positioned within larger commercial structures reliant on immersive advertising and behavioral marketing.
- *Infrastructures:* Enables youth to envision how their social interactions are shaped by the design of the platforms and apps. Privacy management is demarcated by the terms of service, an awareness of default settings that can stifle privacy protective options, and how their ability to meaningfully consent can either be enhanced through understandable language or obfuscated through lengthy legalese.

As young people embrace social media platforms and apps to enhance their everyday sociality and build social capital, and yet are also increasingly required to be online in order to access schoolwork, it is crucial that they comprehend their privacy rights. Navigating and managing their online identities in a commercialized data and information milieu is complex and can be fraught with risks, especially when it comes to grasping platform terms of service and feeling confident that the platform enables them to exercise meaningful consent for their participation. That is why digital privacy policy literacy is so essential for young people.

Acknowledgments

Thank you to the Social Sciences and Humanities Research Council of Canada (SSHRC) for their support of this chapter through two research projects: the Insight Grant, *Opening the Door on Digital Privacy: Practices, Policies, & Pedagogies*; and the Partnership Grant, *The eQuality Project*.

References

Anderson, M. and Jiang, J. (2018, May). *Teens, Social Media & Technology 2018*. Washington, D.C.: Pew Research Center, (no page numbers), http://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018 (accessed 5 January 2019).

boyd, d. and Hargittai, E. (2010). Facebook privacy settings: who cares? *First Monday* 15 (8) https://firstmonday.org/article/view/3086/2589 (accessed 5 January 2019).

House of Commons, Canada. (2018). Democracy under threat: Risks and solutions in the era of disinformation and data monopoly. Report on the Standing Committee on Access to Information, Privacy and Ethics, 42nd Parliament, 1st Session, December. www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf.(accessed 7 January, 2019).

Instagram. (2019a). Why do Facebook and Instagram share information? https://help.instagram.com/833836199971426 (accessed 5 January, 2019).

Instagram. (2019b). How does Instagram decide which ads to show me? https://help.instagram.com/1730813095642229?helpref=faq_content (accessed 5 January, 2019).

Instagram. (2019c). Controlling your visibility. https://help.instagram.com/116024195217477 (accessed 5 January, 2019).

Instagram. (2019d). Privacy settings and information. https://help.instagram.com/196883487377501 (accessed 5 January, 2019).

Instagram. (2019e). How do I share a story with my close friends list on Instagram? www.facebook.com/help/instagram/2183694401643300 (accessed 5 January, 2019).

Johnson, M., Steeves, V., Shade, L.R., and Foran, G. (2017). *To Share or Not to Share: How Teens Make Privacy Decisions About Photos on Social Media*. Ottawa: MediaSmarts http://mediasmarts.ca.proxy.bib.uottawa.ca/sites/mediasmarts/files/publication-report/full/to-share-or-not-share.pdf (accessed 9 January 2019).

Livingstone, S., Stoilova, M., and Nandagiri, R. (2018). *Children's Data and Privacy Online: Growing Up in a Digital Age – an Evidence Review*. London: London School of Economics and Political Science www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf (accessed 9 January 2019).

Office of the Privacy Commissioner of Canada (OPC). (2013). Interpretation bulletin: Personal information. www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/#fn50 (accessed 9 January 2019).

Office of the Privacy Commissioner of Canada (OPC). (2017a). Real fears, real solutions: A plan for restoring confidence in Canada's privacy regime. 2016–17 annual report to parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act. www.priv.gc.ca/media/4586/opc-ar-2016-2017_eng-final.pdf (accessed 5 January, 2019).

Office of the Privacy Commissioner of Canada (OPC). (2017b). Enforcement of PIPEDA. www.priv.gc.ca/biens-assets/compliance-framework/en/index# (accessed 5 January 2019).

Office of the Privacy Commissioner of Canada (OPC). (2018a). What we do. www.priv.gc.ca/en/about-the-opc/what-we-do (accessed 5 January 2019).

Office of the Privacy Commissioner of Canada (OPC). (2018b). About the OPC. www.priv.gc.ca/en/about-the-opc (accessed 5 January 2019).

Office of the Privacy Commissioner of Canada (OPC). (2018c). Privacy Commissioner issues new guidance to help address consent challenges in the digital age. www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180524 (accessed 5 January 2019).

Office of the Privacy Commissioner of Canada (OPC). (2018d). Guidelines for obtaining meaningful consent. www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805 (accessed 5 January 2019).

Office of the Privacy Commissioner of Canada (OPC). (2018e). PIPEDA in brief. www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/#_what_is (accessed 5 January 2019).

Office of the Privacy Commissioner of Canada (OPC). (2018f). Trust but verify: Rebuilding trust in the digital economy through effective, independent oversight. 2017–18 annual report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act. www.priv.gc.ca/media/4831/ar_201718_eng.pdf (accessed 5 January, 2019).

Ouellette, L. and Gray, J. (eds.) (2017). *Keywords for Media Studies*. New York: New York University Press.

Panzarino, M. (2013). Instagram starts showing in feed video and image ads to U.S. users. Tech Crunch. https://techcrunch.com/2013/10/03/instagram-starts-showing-in-feed-video-and-image-ads-to-us-users (accessed 5 January 2019).

Peters, B. (ed.) (2016). *Digital Keywords: A Vocabulary of Information Society & Culture*. Princeton, N.J: Princeton University Press.

RBC Capital Markets. (2017). Internet social butterflies: Highlights from our third social media survey. https://research.rbccm.com/sellside/EmailDocViewer?encrypt=fe696ecc-4007-4584-aaf8-89710eb48b1c&mime=pdf&co=rbcnew&id=dan@splatf.com&source=mail (accessed 5 January, 2019).

General Data Protection Regulation. (2016). Special protection of children's personal data. Recital 38. https://gdpr-info.eu/recitals/no-38.

Rusli, E.M. (2012, 9 April). Facebooks buys Instagram for $1 billion. *The New York Times*. https://dealbook.nytimes.com/2012/04/09/facebook-buys-instagram-for-1-billion (accessed 5 January 2019).

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

Shade, L.R. and Shepherd, T. (2013, December). Viewing youth and mobile privacy through a digital policy literacy framework. *First Monday* 18 (12) https://firstmonday.org/ojs/index.php/fm/article/view/4807/3798 (accessed 5 January 2019).

Smith, K.L., Meisner, K., Shade, L.R. et al. (2015). Co-designing open badges for privacy education with Canadian youth: A project report. https://www-priv-gc-ca.proxy.bib.uottawa.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2014-2015/p_201415_03. (accessed 9 January 2019).

Smith, K.L., Shade, L.R., and Shepherd, T. (2017). Open privacy badges for digital policy literacy. *International Journal of Communication* 11: 2784–2805. https://ijoc-org.proxy.bib.uottawa.ca/index.php/ijoc/article/view/6174 (accessed 5 January 2019).

Snap, Inc. (2017). Registration statement under the Securities Act of 1933. www.sec.gov/Archives/edgar/data/1564408/000119312517029199/d270216ds1.htm (accessed 5 January 2019).

Tunney, C. (2019). Privacy watchdog taking Facebook to court, says company breached privacy laws. CBC News. www.cbc.ca/news/politics/privacy-watchdog-cambridge-analytica-facebook-1.5110304 (accessed 31 July 2019).

van Dijck, J. (2013). *The Culture of Connectivity: A Critical History of Social Media*. Oxford: Oxford University Press.

Wagner, K. (2018). Facebook says millions of users who thought they were sharing privately with their friends may have shared with everyone because of a software bug. Recode. www.recode.net/2018/6/7/17438928/facebook-bug-privacy-public-settings-14-million-users (accessed 5 January 2019).

Wall Street Journal. (2013). Snapchat spurned $3 billion acquisition offer from Facebook. *Wall Street Journal*. https://blogs-wsj-com.proxy.bib.uottawa.ca/digits/2013/11/13/snapchat-spurned-3-billion-acquisition-offer-from-facebook (accessed 5 January 2019).

Williams, R. (1976, new edition, 2015). *Keywords: A Vocabulary of Culture and Society*. NY: Oxford University Press.

Wu, T. (2018). The case for breaking up Facebook and Instagram. *The Washington Post*. www.washingtonpost.com/outlook/2018/09/28/case-breaking-up-facebook-instagram/?noredirect=on&utm_term=.9806b61cc2c4 (accessed 5 January 2019).