Tracing and Tracking Canadian Privacy Discourses: The Audience as Commodity
By Leslie Regan Shade, Concordia University, and Tamara Shepherd, Concordia University

PREPRINT version: May 2012

Published as: Shade, Leslie Regan and Tamara Shepherd. (2014). "Tracing and Tracking Privacy Discourses of Immanent Commodification and Contextual Integrity," in *Publicity and the Canadian State: Critical Communications Perspectives*, ed. Kirsten Kozolanka. Toronto: University of Toronto Press.

At the NextMedia digital media industry conference in Toronto in November 2010, Facebook Canada's managing director, Jordan Banks, told reporters that today's consumers feel it's "their right" to receive targeted advertisements from marketers: "Isn't that the consumer's expectation these days? We're in this era of … this two-way conversation that every consumer feels is their right. Whenever they interact with a brand these days, they want to have a say, they want to be treated personally and they want to be talked to in a timely and relevant manner." While asserting the positive impact of such targeted and branded advertising on Facebook, Banks "downplayed privacy concerns," according to the CBC (Chung 2010). This public disavowal of the threats to privacy by social network sites (social network sites) like Facebook, along with the explicit promotion of targeted ads as a consumer right, demonstrates the way that commodification is immanent to social networking**.** Importantly, it also highlights tensions between the privacy rights of citizen-consumers and their disclosure of and access to personal information in commercial, and highly profitable, social media sites. The right of access to information is the subject of the chapter by Rubin and Kozolanka.

Mosco's (2009) analysis of commodification in the political economy of communication provides a useful and salient entry point into our discussion of how social network sites and other forms of social media have adopted techniques from the marketing sector to create two forms of commodities: the audience commodity and immanent commodification. Commodification **is** understood as taking objects or often non-commercial products and services and transforming them into entities valued for their marketable function and use in exchange processes. It is a phenomenon that has grown in stature and stealth as companies seek to develop and deepen new revenue streams.

The audience commodity, as elaborated by Canadian political economist Smythe (1981b), refers to the processes by which consumers are bought and sold by the media industry. Smythe analyzed how television viewers are constructed by the mass media, arguing that audiences comprise the commodity form of mass-produced, advertiser supported communications under monopoly capitalism. Audiences thus engage in unpaid labour for the media industries by viewing advertisements in their leisure time. Embedded in the costs of ads are the costs of the goods and services that are marketed, which are passed onto the viewer-consumer. This notion of the audience commodity has resonated throughout the years and "has deeply influenced international studies of audience, media and consumption in both cultural studies and political economy. If a commodity, the audience is hardly sovereign" (C. Murray 2010, 84). The audience

commodity is a huge industry, comprising the media companies themselves, the advertisers that are attracted to specific media products and the particular demographic they can target, and the groups that track the impact of advertising on its viewers.

Newer offshoots of marketing online—involving psychographics, demographics, and behavioural advertising—are constitutive of what Mosco (2009, 143) calls "immanent commodification": the processes wherein the audience commodity, in fact, produces new commodities. This involves the interrelatedness of multiple practices that produce incremental levels of exchange value, and particularly those that create

> new measurement and surveillance technologies to expand the production of media commodities. Internet cookies, digital television recording devices, 'smart' cards, etc., produce new products, in the form of reports on viewing and shopping, containing demographic details that are linked to numerous databases. But these new products are more than discrete units. They are part of a commodification process that connects them in a structured hierarchy. The implications for privacy are powerful. […] *Immanent commodification not only produces new commodities; it creates powerful surveillance tools that threaten privacy* (Ibid., our emphasis).

Nissenbaum's (2004) notion of "contextual integrity" and its impact on informational privacy is also key to our discussion. Nissenbaum argues that contextual integrity—the various informational contexts that govern or habituate privacy norms—should be considered the benchmark of privacy. Privacy violations are comprised of variables that are situationally dependent, including "the role of agents receiving information; their relationships to information subjects; on what terms the information is shared by the subject; and the terms of further dissemination" (137-8). Contextual integrity is used to explain our increasing unease with pervasive forms of public and covert surveillance, especially with increasingly ubiquitous computerization regimes that tend to outpace the development of policy that protects privacy rights. Such developments again draw attention to a shifting privacy-information rights dichotomy.

As threats to citizen rights of online privacy, immanent commodification and contextual integrity on social network sites have been central to recent policy discussions that explore whether federal privacy legislation has kept pace with technological developments. This chapter looks at several policy papers from the Office of the Privacy Commissioner of Canada (OPC) and the consumer organization, the Public Interest Advocacy Centre (PIAC). These recent papers have roots in much earlier concerns around the emerging landscape of information technology in Canada, as computers were introduced into the work practices of governments and corporations amidst the creation of 'databanks' containing citizens' personal information.

In this chapter, we situate recent Canadian policy documents from the OPC and PIAC in light of their predecessors, the *Instant World* (Canada 1970) and *Privacy & Computers* (Canada 1972) reports issued by the now defunct Department of Communication. These earlier reports also raised privacy concerns, long before social network sites such as Facebook came to define what we take for granted today as mundane forms of everyday social networking. Here, we explore how the notions of immanent commodification and contextual integrity have been conceptualized and treated as policy issues—where regulation tends to lag behind technological innovation—

throughout the intensification of networked communication over the last forty years.

The Context of Canadian Privacy Legislation

Issued in the early 1970s by the Department of Communication, *Instant World: A Report on Telecommunications in Canada* (1970) and *Privacy & Computers* (1972) examined the integrity of personal information and the potential surveillance implications of nascent database technologies for sorting, tracking, and making links by governments and private industries, alongside concerns about the outsourcing of Canadian data to the detriment of national sovereignty. *Instant World* originated from the Department of Communication's Telecommission, a two-year comprehensive study of the socio-economic and political impact of telecommunications in Canadian society. The report was prescient in its predictions of the widespread use of telecommunications technologies for society, and concluded that "the establishment of a Canadian right to communicate was required in order to confront the social implications of the ever-increasing centrality of technologically mediated communication to Canadian society" (Raboy and Shtern 2010, 4). *Privacy & Computers* stemmed from a joint task force of the departments of Communication and Justice. Ten major discussion papers were commissioned by government and from independent experts, including overviews of the privacy implications of new technologies, the increased information-gathering and processing roles of governments and corporations, security safeguards, the regulatory role of governments, law enforcement agencies, and the effect of constitutional protections. In response to these early regulatory concerns both the OPC and PIAC were established.

The OPC was created with the passing of the Canadian *Human Rights Act* in 1977 to serve as an advocate for the privacy rights of Canadians whose personal information was stored in federal databanks. It is headed by a Privacy Commissioner, appointed for a seven-year term by the Governor General on the recommendation of Cabinet. The Privacy Commissioner's powers include: investigating complaints, conducting audits and pursuing court action under the two pieces of federal privacy legislation, the *Privacy Act* (1983) and the *Personal Information Protection and Electronic Documents Act* or *PIPEDA* (2000); reporting on public and private sector organizations that handle personal information; conducting and publishing research on privacy issues; and engendering public awareness of these issues.

The *Privacy Act* applies to the federal public sector related to data collection, and places limitations on the collection, use, disclosure, and disposal of personal information held by the federal government and federal agencies (Canada 1982, 1983). *PIPEDA* applies to the federally regulated private sector with respect to the collection, use, and disclosure of personal information, but only for the transaction of commercial activities (Canada 2000). Jennifer Stoddart, commissioner from 2003 to 2013, has been a global leader for her strong stance in demanding accountability in the privacy practices of popular social media companies, such as Facebook and Google, and in advocating for public education on digital privacy, particularly for young people (McNish 2010).

While the privacy commissioner is an Officer of Parliament, and thus represents an arm of the federal government, PIAC is a non-profit organization**.** Founded in Ottawa in 1976, it provides legal and research services around consumer rights, especially the interests of vulnerable (i.e. low-income) consumer groups in procuring access to critical public services. In responding to the challenges of fulfilling such an ambitious mandate in

the context of a small non-profit organization, PIAC (2001, 7) expressly limited its purview in the 1990s to telecommunications, the Internet, energy, privacy, and competition law. Additionally, earlier courtroom activities of PIAC have since shifted to primarily research-based models of consumer advocacy, according to the principle that "public policy is best determined when all elements of the public interest are represented by informed advocates at the time decisions are made" (32).

Thus the OPC and PIAC were formed with different mandates, yet the two organizations have recently adopted similar concerns over how immanent commodification might threaten citizens' right to online privacy. Social network sites have received particular attention, for example, in the OPC's 2009 report, *Social Network Site Privacy***,** and its 2010 public consultations on the practices of online tracking, profiling and cloud computing,[1] in light of the mandated five-year review of *PIPEDA* in 2011. In compiling its final report based on these public consultations and with input from written stakeholder submissions, the OPC focused primarily on "behavioural advertising"—another term for the online tracking of user behaviour as part of a marketing strategy (Stallworth 2010). In evaluating the merits and limitations of *PIPEDA* in this context, the review also influenced the OPC's submission to the federal government's Digital Economy Consultation in July 2010, where it emphasized the need to conduct new research on areas of vexing privacy concerns. One of the main areas relevant to our discussion in this chapter reflects the immanent commodification of personal information online, particularly on social network sites.

The OPC's recommendations to the federal government on how to deal with SNS privacy take a standpoint similar to recent PIAC reports. Since 2004, PIAC has compiled policy research on the effectiveness of *PIPEDA* in protecting consumer privacy online in relation to practices such as third-party advertising, target marketing, and online behavioural tracking, and how these various iterations of immanent commodification pose special risks to children and minors. While PIAC tends to use qualitative methodologies including surveys, focus groups and interviews, many of its conclusions about the need for increased privacy protection resemble those from the OPC on the commodification of personal information online.

Moreover, both organizations tend to reproduce some of the older discourses around privacy in relation to changing technology as expressed in *Instant World* and *Privacy and Computers*. Indeed, the concerns enumerated forty years ago are still with us now, but are exacerbated with the popular increase in social media over a wide demographic—from young people to middle-aged adults—along with more complicated data-based practices such as deep packet inspection (DPI),[2] cloud computing, and behavioural tracking.[3] The next sections show clearly how early conceptions of informational privacy gave way to later discourses expressing heightened tensions about the impact of commercialization in online environments on the privacy rights of citizen's personal information.

Early Discourses: Concerns over Informational Privacy and a Right to Privacy

Informational privacy as a societal concern became a topic of prevalent public discourse in the 1960s, as computerization entered the management of government and corporate activities. Reporting on a series of public forums preceding the release of *Instant World*

in 1970, the *Globe and Mail* conveyed concerns that widespread computerization would "'mak[e] us the greatest data-generating, privacy-invading society ever known'" (Sagi 1970, B7). Another news article summarized that "nosy people have always been a nuisance, in the society that values privacy. If they are permitted to enlist the full support of computers, such people could soon become a major threat to Canada's open, democratic life style" (Braithwaite 1970, B2). The article further reported on a proposal for a right to privacy made by A.E. Gottlieb, Deputy Minister of Communication, who warned that if this right was not established, "power will increasingly flow to those who know how to manipulate electronic information systems," and that "with electronic memories it will be possible to collect all possible data on a given individual and this body of information will follow him [sic] throughout his life like a ball and chain" (Ibid).

Instant World categorically called for the consideration of a "right to privacy," given the rapid uptake of information technologies to collect, store, manipulate, and distribute information. While acknowledging the "administrative economies" enabled by these new applications, the report cautioned against the discriminatory use of technologies to the detriment of citizens' privacy, especially for more vulnerable members of society (Canada 1970, 41).

Privacy & Computers similarly detailed the technical, administrative and legal challenges of the mounting collection of personal information and its resultant privacy issues: accuracy and integrity of data; right of access to personal information; and the relationship between information, privacy and political power. The preponderance of privacy concerns, the report noted, resided in the uncertainty about the extent of these new power structures, but noted that informational privacy was "in essence, a political and not a legal issue" (Canada 1972, 19).

The report further cautioned against "presentiment[s] of a technocratic nightmare" through government and corporate misuse or abuse of information (119, 120) and acknowledged concerns surrounding the collection of personal information, its accuracy, dissemination to third parties, and the right of individuals to access and verify the integrity of their personal information. A "right to privacy" was thus seen as a widespread social claim with respect to personal information.

Contemporary Discourses: Contextual Integrity

Earlier concerns over the context of information disclosure have proved prescient, as shown in the OPC's *Social Network Site Privacy* report, which applies Nissenbaum's (2004, 2010) notion of "contextual integrity" to describe how privacy legislation is only meaningful and effective within the context of users' expectations (see also Grimmelmann 2009). Echoing early debates around a "right to privacy" as an individual matter, Nissenbaum (2010, 236) frames contextual integrity as a concept that seeks to establish "whether socio-technical devices, systems, and practices affecting the flow of personal information in a society are morally and politically legitimate." While she cautions that contextual integrity is neither a legal right nor a legal concept of privacy, she argues that it is still useful for providing a standard for evaluating privacy legislation according to users' expectations.

It is important to note that these expectations develop not through the state's regulatory paradigms, but rather through community norms in online spaces for social networking. Privacy violations are thus recognized as breaching one of two main types of

norms: “the norm of what information is appropriate to collect, and the norm of how information flows and whether it is appropriate to distribute that information” (OPC 2009a, 5). Some of the challenges of this definition of privacy as norms-based include differentiating between public and private (as noted in earlier reports from the Department of Communication), but also the conundrum of determining users’ attitudes toward social network sites as particular sites for communication. As the **OPC** report argues, users of Social network sites partake in an “illusion of privacy” furnished by the controls they exert over who can see their profiles among their network of friends, without a clear understanding of how their informational privacy is breached by immanent commodification, especially through the less visible collection and use of their personal information for commercial purposes (OPC 2009b, 6).

The concept of contextual integrity is useful when extending definitions of privacy to newer technologically mediated spaces for communication like social network sites, but it also bears upon older and ongoing concerns for policymakers in this area. In *Privacy in a Changing Society* (OPC 2010b, 3), the OPC names four central and interrelated issues that affect privacy legislation: information technology, the integrity of personal identity, genetic information and national security. The first two concerns—information technology and the integrity of personal identity—most obviously emanate from the immanent commodification challenge of Internet technology, where the profitability of networked communication poses threats to the security of personally identifiable information.

In less apparent ways, national security is also implicated in concerns around privacy as contextual integrity. National security mandates often work in tandem with commercial data mining initiatives. For instance, the report highlights the increased challenge to privacy legislation from “ubiquitous computing,” where every object and living thing (including people) can be tagged through technologies like radio-frequency identification (RFID). In this scenario, one can imagine the integration of genetic data into personal data profiles that cannot be controlled or managed by individuals themselves, which then not only breaches the integrity of personal identity and personal information, but heightens surveillance and security mechanisms by government and corporate interests.

A series of consultations held in 2010 by the OPC also summarizes various concerns relating to privacy as contextual integrity. The three touchstone issues discussed in the consultations—tracking, profiling and targeting, and cloud computing—likewise invoke the notion of immanent commodification, especially since most of these technological advances have emerged from the marketing sector. The report based on these consultations notes that the convergence of online information has built up increasingly complete portraits of individuals, using their personal information without their explicit knowledge, consent or control, thus creating an audience commodity. Alongside the fraught nature of tracking and profiling, protecting people’s privacy presents a more complex challenge to participating in online life altogether (OPC 2010c, 14). In taking a more holistic approach to technologically mediated behaviours, the report invokes both the ideas of contextual integrity and immanent commodification. Because privacy is contextually dependent, where the context is always already inscribed within capitalist business practices, the OPC acknowledges the need to have privacy protections built into system defaults to meet basic regulations (OPC 2010d, 15).

It is apparent to us, and indeed to the OPC, that the issues of contextual integrity and immanent commodification represent a case of "new technologies, old questions" (Ibid., 5). The *Instant World* and *Computers and Privacy* reports from the 1970s cautioned about power imbalances between the rights of individuals to protect and control their personal information (particularly the more vulnerable in society) and large governments and corporations that sought citizen information for administrative task-making and potential consumer profiling.

Yet there are qualitative changes to the flow of data across networked spaces. As such, while the OPC boasts that Canada is a world leader in privacy protections—citing our progressive legislation, such as the *Human Rights Act* (1977), *The Charter of Rights and Freedoms* (1982), *The Privacy Act* (1983) and *PIPEDA* (2000)—federal regulation has not kept pace with technological innovation (OPC 2010a, 4). Especially with regard to immanent commodification, the OPC has argued, users' lack of control over their unintentional virtual profiles fundamentally reduces expectations of privacy, in effect automatically waiving privacy rights online (OPC 2008, 5). In addition, while Canada has no explicit recognition of privacy as a human right, there are court precedents for assuring a "reasonable expectation of privacy"; however, the spontaneous and peripatetic nature of transactions and communicative flows on social network sites renders the establishment of such "reasonable expectations" vexatious (Shade 2008).

Immanent Commodification and Privacy on Social Network Sites

Earlier policy documents primarily envisioned computers as facilitating the workflow of administrative functions through the creation and cross-referencing of private citizens' information in databases, a necessary bureaucratic function. Maintaining both the integrity of database information and allowing citizens to redress erroneous information was deemed essential. Safeguarding personal information, thus protecting the informational sovereignty of Canadians, was also a major concern with the increase in transborder data flows.

Since this time, as the OPC's report on online tracking notes, the introduction of the *Privacy Act* (1983) sought to protect personal information in government databanks, while *PIPEDA* (2000) addressed concerns around commercial threats to individual privacy in a changing technological landscape. Yet, despite its attempt at technological neutrality, *PIPEDA* has not even managed to keep pace with the ever more sophisticated iterations of immanent commodification online within the ten years since it was drafted. As the 2004 Public Interest Advocacy Centre review of *PIPEDA* found only three years after it was enacted, the earliest adopters of its complaint-resolution system displayed a lack of consistent complaint filing and resolution, stemming from the lack of an effective enforcement mechanism (PIAC 2004, 13). Consent was identified as the key problem in these cases, as articulated in Principle 3 of *PIPEDA*: "The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate" (*PIPEDA* 2000, n.p.). PIAC's report contends that this wording is vague and unclear, leaving online commercial actors free to assume implied consent across numerous situations of information collection.

In addition to the lack of a clear consent requirement, *PIPEDA*'s effectiveness is compromised by its position as a statute tacked onto the *Privacy Act*, rather than being enshrined within that Act (14). Immanent commodification of personal information thus

escapes proper scrutiny as a violation of fundamental privacy rights—a violation that implicates not only corporate collection and use of personal information, but that of government agencies as well. As the Federal Trade Commission emphasized in its report on consumer privacy protection in the United States, corporations should look to government models for handling personal information in determining the "privacy impact of specific practices, products, and services" (FTC 2010, 49). In the Canadian context, this would involve strengthening *PIPEDA* reviews to include reviews of the *Privacy Act* and the *Criminal Code* (1985) as well, since the federal government should serve as a "model user" for enforcing legislated privacy protections, thus gaining citizen trust (OPC 2010b, 12).

Critiques of existing privacy legislation, especially *PIPEDA*, stem not only from the shortcomings of the *Act*, but also from technological changes that outpace the development of federal regulation. As PIAC (2009, 18) notes in its report on the possibility of a Do Not Track List for Canada,[4] pre-Internet models for commodifying people's information relied on demographic segmentation, psychographics, and offline data mining—for example, in companies' computer systems about their consumers—but today, data mining has become easier and more sophisticated with e-commerce and online surveillance technologies based on tracking consumer behaviour on the Internet. This unregulated arena has a profound impact on commodification. Industry spending on behavioural tracking is estimated to be in the many billions and growing (PIAC 2009, 19), to which the OPC (2010c) has enumerated concerns that these expansionary "dataveillance" practices intrude into formerly private domestic spaces as individuals increasingly participate in commercial activities from their home computers (6). In this way, immanent commodification has accelerated the spread of intrusive marketing practices such as tracking, while qualitatively changing and challenging the notion of a public-private boundary.

New and refined technologies are key to how immanent commodification poses threats to people's contextual expectations of privacy. OPC consultations on online tracking, targeting and profiling solicited respondents' opinions on how information might be collected via cookies, log files and deep packet inspection (10). These mechanisms were associated with practices such as surveillance, dataveillance, mapping, monitoring and geo-tagging—all able to amass personal data within only a small number of commercial and governmental organizations. This concentration of users' information incorporates relatively new sources of personal information including social network site (SNS) profiles that can be arranged in data clouds (OPC 2010a, 7).

The OPC notes that new mechanisms, practices and modes of data collection and storage occur in social network sites primarily concerned with advertising, but also across many other business models: mapping technologies that integrate street-level information with data storage; location-based services for marketing and Internet search; the "Internet of things," a term that describes a host of new means of rendering objects and persons as data through advanced internetworking technologies, including sensor networks, Internet Protocol version 6, RFID tags, wireless sensors, smart technologies and nanotechnologies; analytics like databases and algorithms; e-Health modules containing personal health records; and newly evolving business models based on Web 2.0, third-party applications and cloud computing (7-10). In all these scenarios for data collection, immanent commodification implies that the creation of virtual profiles based on people's

information happens without their control or even knowledge, with audiences for such profiles including data brokers, marketers, investigators, monitors, and identity fraud scammers (OPC 2008, 4).

Within this broad span of data collection and usage practices online, social network sites present unique challenges to legislated privacy protections, particularly because they are online spaces that invest users with the *perception* of control over their online profiles. While such intentional profiles are only "the tip of the iceberg" when it comes to data-based personal profiles online (1), users of social network sites perceive their rights to participate in these networks from the standpoint of social privacy (i.e. who can see their profile among the network) rather than informational privacy (i.e. marketers and other third-party organizations accessing their own information).

This apparent elision of informational privacy on social network sites is crucial in allowing the sites to operate according to advertising revenue models. Advertising allows these sites to offer services for free, where user information helps marketers to target ads to users' interests, and to "inject themselves into conversations and manipulate participants into being favourably disposed towards their products by using loyal consumers' word-of-mouth to communicate a firm's bottom-line to new prospects" (PIAC 2009, 42). As Facebook Canada's Jordan Banks claims in the CBC story quoted at the beginning of this chapter, consumers welcome this "very targeted and relevant and personalized messaging" as part of developing "very meaningful and rich relationships with brands" (Chung 2010). However, online tracking on social network sites like Facebook pose potentially serious privacy risks. These risks clash with the ideals of Facebook CEO Mark Zuckerberg's belief in "radical transparency"—the company's credo that creating more open and transparent identities creates a healthier society (Kirkpatrick 2010).

But this sense of "radical transparency" is also elitist. For many people, the ability to control and maintain one's personal privacy on social network sites implies a particularly high level of information literacy, especially as privacy controls and features change continually at the seeming whim of technology designers, who tend to claim that these changes are implemented for the user's benefit. In this sense, privacy becomes, as Papacharissi (2010, n.p.) characterizes, a "luxury commodity," one that only those with higher socio-economic and cultural capital can regulate. There is a risk, she cautions, of a privacy divide "further enlarged by the high-income elasticity of demand that luxury goods possess" between those who can "afford greater access to privacy" and those who can't—a newer class of "have-nots." Papacharissi's comments are redolent of *Instant World*'s cautions to ensure that privacy rights do not remain elitist, and to be attentive to the "less powerful" in society, "welfare recipients, the out-patient at a public clinic, or the indigent senior citizen" (Canada 1970, 42).

Considering Facebook's reliance on "transparency" as an ultimately fallacious way of granting users control over their personal information**,** the OPC report on social network privacy (2009b) contends that social network sites are particularly prone to placing users' privacy in danger. As the report details, privacy policies on these sites are required by *PIPEDA* to include transparent statements about how information is collected and used.[5] Yet, even with increased transparency in privacy policies, relationships between social network sites and advertisers often remains unclear; this occurs alongside the vague process of aggregating information so that it is not "personally identifiable"

(45-46).

Expanding the OPC's recommendations for clearer wording, PIAC has suggested that Canada implement a Do Not Track List, which has been proposed in the US by the FTC as "a universal mechanism" through legislation or self-regulation (FTC 2010, 66). Such a mechanism would allow users to bypass the numerous privacy threats posed by the collection and use of personal information on social network sites: compromised transparency; implied consent; little or no control over opting out; opt-out consent as the main model rather than opt-in; the selling of information to third parties; the packaging and aggregation of data in data mining operations; incomplete or impermanent anonymization of personal information; and more generally, the ways that online profiling can discriminate and lead to loss of consumer autonomy through predictive models of behaviour (PIAC 2009, 49-53).

Particularly troubling about the range of privacy threats on social network sites is their use by and appeal to children and youth under the age of majority. Canadian privacy legislation includes no special laws related to the protection of minors' personal information online against commercial breaches of privacy. Children's information is an especially sensitive category of personal data, amplifying threats of misuse and abuse. Children may also disclose personal information more readily to commercial sites posing as games, termed "immersive advertising" (PIAC 2008, 23), or on sites where ads are indistinguishable from its content (2009 54-5).

Moral panics about online predators have overshadowed these informational privacy threats, with federal privacy regulation containing little protection over minors' personal information. In the US, the 1998 *Children's Online Privacy Protection Act* aims to safeguard the informational privacy of children under the age of 13, mainly through putting the onus on parents rather than on the sites themselves to make sure kids understand how to protect their information online. In practice, it is relatively easy for young Internet users to circumvent their parents' discretion and use social network sites by claiming an older birth date (PIAC 2008, 32). Even though Facebook requires new users to be over the age of 13, children still create profiles and use the site for social interaction—accepting the conditions of data collection and use as specified in its Terms of Service and Privacy Policies, arguably without being able to give meaningful consent (Burkell, Steeves, and Micheti 2007).

Conclusion: Privacy as User Control of Personal Information

In the reports from the 1970s, as well as today, the primary objective of policy research in Canada has been to suggest recommendations to policymakers on how to effect legislation to protect citizens' rights more comprehensively. In regard to privacy in online social networks, recommendations from the Office of the Privacy Commissioner and the Public Interest Advocacy Centre focus on amendments to *PIPEDA*, reflecting the concern with immanent commodification in the private sector's collection and use of personal data. Yet in a more general sense, as indicated by the *Instant World* and *Privacy & Computers* reports issued long before *PIPEDA* was drafted, regulation needs to invest citizens with control over their own data online. As part of Nissenbaum's characterization of privacy as contextual integrity, control over personal information—the ability to determine what information gets collected and used in certain contexts—is critical for upholding privacy as a fundamental right of citizenship.

A first step for granting users more control over their own personal information is mandating websites to draft transparent Privacy Policies to increase public understanding of how online platforms collect and use personal information. On social network sites, for instance, the OPC (2009b, 47) would require the sites to provide a clearer and comprehensive explanation of how personal information is collected and used. PIAC (2009) reiterates the importance of transparent privacy policies, and suggests that companies should detail the following information for users:

> 1) what personal information about them is collected, and especially what sensitive personal information is collected (e.g., health and financial information);
> 2) how this information will be used for online behavioural targeted advertising;
> 3) how long this information will be retained by the website operator and/or the parties with which they share the information; and
> 4) to whom this information will be disclosed, including affiliates and third party marketers and market researchers. Definitions should be provided for "affiliates," "third party" and "partners" (75).

The rationale behind standardizing privacy policies is to ensure that they describe exactly how personal information gets collected and used, in order to improve the reliability of informed consent (75). The argument is that if policies offer users more transparency, the result will be increased understanding of data flows online, enabling users to grant more meaningful consent.

In addition to exercising their capacity to give informed consent through transparency of privacy policies on social network sites and other commercial web platforms, the OPC (2010a, 17) recommends that users apply a number of identity management tools. These rest on a similar rationale for meaningful consent, where users should know never to disclose key identifying information in online contexts (such as Social Insurance Number, date of birth, address, and phone number). Moreover, they should be aware of how their information is used on sites, not only through reading complex privacy policies, but through a more general understanding of how marketing works on seemingly "free" websites like social network sites (OPC 2008, 6).

If these requirements for users seem somewhat vague and demanding, PIAC has taken a different approach from the OPC in developing privacy management tools. Following the US Federal Trade Commission's discussion papers on a Do Not Track List, PIAC suggests that a similar mechanism might be adopted effectively in Canada. The main benefit of such a list would be to absolve consumers' responsibility to file a complaint if they feel their rights are being breached (PIAC 2009, 71). And while the barriers to implementing such a list include legal, operational, technological, monetary and social constraints, PIAC's (Ibid., 72-7, 76) survey respondents supported the idea of a Do Not Track List, especially since it does not depend on complaint resolution as the main mechanism for federal privacy regulation.

But federal regulatory amendments such as a Do Not Track List need to be drafted in consideration of broader global privacy legislation. Recalling the issue of transborder information flows central to the much earlier *Instant World* and *Privacy & Computers* reports, PIAC's interest in the American regulatory debates indicates the importance of internationally minded revisions to existing legislation. In that regard, PIAC references American and European Union research on potential changes to

PIPEDA's complaint resolution framework. They argue that *PIPEDA* should be used to more reliably enforce the privacy safeguards in transnational business models based on secondary marketing (PIAC 2004, 3).

While the OPC has not always been willing to examine *PIPEDA*'s flaws, it has also suggested potential legislative alterations in line with the international regulatory community. In an online context where state borders are more contingent—a dimension of networked technology that has only become amplified since the 1970s—federal privacy protections need to eliminate what the OPC (2008, 3) calls "jurisdictional uncertainty." The OPC has thus been following the International Standards Organization in determining how to set up more secure models for online transactions involving data, in a climate where "citizens want to know that privacy protections are in place, and businesses want to have a common set of rules to follow" (5). Likewise, the first privacy protection recommendation put forth by the OPC in the federal government's 2010 consultations on Canada's digital economy strategy emphasizes that any amendments to PIPEDA must underscore global flows of data by implementing privacy controls for users from the design stage of technological and business model development (OPC 2010a, 11).

Yet regulatory methods of granting control over their personal information to citizens face several challenges related to the immanent commodification of personal information online. Internet businesses like social network sites often depend on data transactions for generating profit (Campbell and Carlson 2002), and as such, these companies are reticent to draft more transparent Privacy Policies or grant users more robust privacy controls. Moreover, as discussed above, increased transparency and privacy management tools assume a baseline level of privacy literacy on the part of citizens, making privacy a "luxury commodity" (Papacharissi 2010) in a context where publicity becomes cheap. To this end, a key element of the OPC's recommendations concerns research on and implementation of public education programs to encourage privacy literacy. Such programs face the challenge of effective implementation given that responsibility for education in Canada lies at the provincial level and there is no federal department for education (Whitehead and Quinlan 2002, 14).

Perhaps, as the OPC's report on SNS privacy proposes, the most effective means for transmitting awareness of privacy rights to citizens is through the viral spread of information on social network sites themselves. In this regard, the development of online privacy management tools should be accompanied by "finding ways to normalize privacy choices within the SNS context so that not only those who are currently using SNS actively engage with them but so that as new users join, privacy becomes as viral as other behaviours" (OPC 2009a, 6). Yet these viral means are both difficult to manage and peripheral to the key issue of ensuring that users exercise meaningful consent, especially when it comes to younger users of SNS and similar web platforms. The OPC has identified children as requiring special attention in this regard, particularly on immersive advertising sites, submitting a revision to *PIPEDA* that would require a "reasonable" expectation that users understand how their information is being collected and used (OPC 2010c, 19). This vague stipulation on the responsibility of the sites to define the validity of consent represents but one side of the premise of individual understanding.

As part of the other side—privacy education and literacy—the OPC has attempted to inform young people about their privacy rights through their youth-oriented website

Youthprivacy.ca. The site features bright colours and the logos MyPrivacy, MyChoice, MyLife amidst iPod-advertising-inspired action silhouettes of young people dancing, jumping, and kick-boxing. Its modules include an interactive MyPrivacy Quiz, an overview of how to manage one's own privacy, an explanation of privacy legislation and the operations of the OPC, along with information on what to do about privacy breaches from peers or websites. A blog updates privacy events and issues, and highlights the annual 'My Privacy and Me' National Video Competition for short youth-produced videos about personal privacy. Winning submissions, judged by a youth panel, are available on the OPC website and the PrivacyComm YouTube channel (OPC 2008, 6).[6]

The impact of YouthPrivacy.ca in shaping young people's knowledge of online privacy and immanent commodification online has not yet been assessed. An alternative educational approach is forwarded in PIAC's report *All in the Data Family* (2008), which proposes stringent recommendations for how social network sites themselves communicate their marketing practices to young users. Alongside the report's contention that SNS privacy defaults should reflect the most *closed* rather than open settings, it also calls for the development of a specific set of guidelines for children and minors in different age groups with an increased onus on the sites to implement these, along with higher standards of privacy protection. The report recommends legislation prohibiting the collection, use and disclosure of all personal information from children under the age of 13, consent from both teen and parent for 13- to 15-year-olds, and just the teen's consent for young people aged 16 to the age of majority at 18 or 19, depending on the province. Once the teen does reach age of majority, PIAC recommends that all their previously stored online data be wiped clean (4-5).

PIAC's approach to privacy protection for young users is thus instructive for privacy regulation more generally. Since it is easier to conceptualize the threat of immanent commodification when discussing children's use of SNS platforms, the recommendations around the collection and use of their personal information tend to be more comprehensive and urgent. This urgency ought to be applied to privacy protections for all citizens, especially considering the OPC's stated contention that "the social transformation that has taken place in the span of a single generation due to the Internet is nothing short of staggering" (OPC 2008, 7).

The panoply of popular social media tools—Internet technologies that allow for participative communicative practices wherein users can develop, collaborate, customize, rate and distribute Internet content—pose particular policy challenges. Our concern in this chapter is privacy, especially related to the protection of personal information, the covert pervasiveness of third-party marketing, and informational integrity. Related concerns include protection against illegal and inappropriate content, promoting and preserving freedom of expression, and security and safety.

Social network sites enable what Christensen (2009, n.p.) terms "complicit surveillance," in what seems to be a growing cultural acceptance that such sites are a legitimate means for corporations, employers and the public to monitor the personal communication of citizens. Christensen comments that the often naïve yet enthusiastic uptake of these technologies "is giving way to a new surveillance, where the act is consensual and guilt (of convenience and pleasure with a cost) shared." The sophisticated search algorithms and data mining software activated on these participatory platforms exemplify immanent commodification. Hence, an attention to the tenets and parameters

of contextual integrity is key to this milieu. Privacy should not have to be a luxury that only the more knowledgeable members of society can lay claim to, nor should it be a commodity that gets shaped by the logic of supply and demand. A truly radical initiative would be to make sure that privacy rights become intrinsic to communication rights alongside access to information.

Endnotes

1. Cloud computing is defined by the OPC as "the provision of web-based services, located on remote computers, that allow individuals and businesses to use software and hardware managed by third parties. Examples of these services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available" (OPC 2010a).
2. DPI involves the use of network management tools to investigate the digital packets that comprise an electronic message or its transmission over a network. While typically used to ensure the security and integrity of the network, DPI can be used to infringe on users' personal privacy by facilitating third parties' ability to look into the content of messages, thus allowing for the targeting of personalized marketing messages (OPC 2009b).
3. Behavioural tracking is a "surreptitious tracking and targeting" of the online transactions of users, including their search queries, social network site content, web pages visited, e-mail content and mobile phone location. Content is culled and analyzed to create targeted and ostensibly "relevant" advertising (Center for Digital Democracy 2009).
4. Unlike a Do Not Call List for avoiding telemarketers, which relies on the federal government compiling a national registry of identifying telephone numbers, the proposed Do Not Track List would entail a browser-based system being made available to citizens. This system would run through browser cookies, indicating to behavioural marketers that they may not collect that user's information. As the FTC notes, one of the many potential challenges of implementing this system would be its reliance on self-regulation by marketers (FTC 2010, 66-67).
5. Facebook was found to violate several of *PIPEDA*'s principles, as detailed in a comprehensive complaint filed by students at the University of Ottawa's Canadian Internet Policy and Public Interest Clinic (CIPPIC 2008).
6. See http://www.youtube.com/privacycomm?gl=CAandhl=enandhl=en and a video produced by the OPCC about their youth initiative at http://www.youtube.com/watch?v=eH6t20mlMVE and on Social network sites at http://www.priv.gc.ca/information/social/index_e.cfm.

Acknowledgements

This paper has been written thanks to the generous funding from SSHRC for the research project *Young Canadians, Participatory Digital Culture and Policy Literacy.*

References

Braithwaite, Chris. 1970. Invasion of Privacy is Feared From Computer Manipulation. *The Globe and Mail*. 23 May, B2.

Burkell, Jacquelyn, Valerie Steeves, and Anca Micheti. 2007. *Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand.* Ottawa: Privacy Commissioner of Canada. http://www.idtrail.org/files/broken_doors_final_report.pdf. Retrieved April 2, 2011.

Campbell, John Edward, and Matt Carlson. 2002. Panopticon.com: Online Surveillance and the Commodification of Privacy. *Journal of Broadcasting & Electronic Media* 46, no. 4: 586-606.

Canadian Internet Policy and Public Interest Clinic (CIPPIC). 2008. PIPEDA Complaint: Facebook. Filed 30 May. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.121.4912&rep=rep1&type=pdf Retrieved April 2, 2011.

Center for Digital Democracy. 2009, September. Online Behavioral Tracking and Targeting: Legislative Primer. *Center for Digital Democracy*. September. http://www.democraticmedia.org/doc/privacy-legislative-primer/ Retrieved April 2, 2011.

Christensen, Miyase. 2009. Watching Me Watching You: Complicit Surveillance and Social Networking. *Le Monde Diplomatique*. October. http://mondediplo.com/2009/10/02networking#nb2. Retrieved April 2, 2011.

Chung, Emily. 2010. Consumers want targeted marketing: Facebook. *CBC News*. 30 November. http://www.cbc.ca/technology/story/2010/11/30/facebook-targeted-marketing.html#ixzz16tAgLH3q. Retrieved April 2, 2011.

Department of Communication. 1970. *Instant World: A Report on Telecommunications in Canada*. Ottawa: Government of Canada.

Department of Communication/Department of Justice. 1972. *Privacy & Computers*. Ottawa: Information Canada.

Federal Trade Commission (FTC). 2010. *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*. Washington DC: Federal Trade Commission.

Government of Canada. 1977. *Canadian Human Rights Act*. Ottawa: Canadian Human Rights Commission.

Government of Canada. 1982. *Charter of Rights and Freedoms*. Ottawa: Government of Canada.

Government of Canada. 1982. *The Privacy Act* (R.S., 1985, c. P-21). http://laws.justice.gc.ca/en/p-21/index.html. Retrieved April 2, 2011.

Government of Canada, 2000. *Personal Information Protection and Electronic Documents Act* (2000, c.5). http://laws.justice.gc.ca/en/P-8.6/index.html. Retrieved April 2, 2011.

Grimmelmann, James. 2009. Saving Facebook. *Iowa Law Review* 94: 1137-1206.

Kirkpatrick, David. 2010. *The Facebook Effect: The Inside Story of the Company That is Connecting the World.* NY: Simon & Schuster.

Lindsay, John V. 1967. Our Precious Right to be Unheard: The Invasion of Privacy. *Life* Magazine: 19, 6 October.

McNish, Jacqui. 2010. Jennifer Stoddart: Making Your Privacy Her Business. *The Globe and Mail.* 10 December. http://www.theglobeandmail.com/report-on-business/managing/the-lunch/jennifer-stoddart-making-your-privacy-her-business/article1833688/singlepage/#articlecontent. Retrieved April 2, 2011.

Mosco, Vincent. 2009. *The Political Economy of Communication, Second Edition*. Thousand Oaks, CA: Sage Publications.

Murray, Catherine. 2010. Audience-Making: Issues in Canadian Audience Studies. In *Mediascapes: New Patterns in Canadian Communication, Third Edition*, ed. Leslie Regan Shade, 83-103. Toronto: Nelson Canada.

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Nissenbaum, Helen. 2004. Privacy as Contextual Integrity. *Washington Law Review* 79, no. 1: 101-139.

Office of the Privacy Commissioner of Canada (OPC). 2010. *Draft Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting and Cloud Computing*. Ottawa: Office of the Privacy Commissioner.

Office of the Privacy Commissioner of Canada (OPC). 2010a. *Privacy in a Changing Society*. Ottawa: Office of the Privacy Commissioner.

Office of the Privacy Commissioner of Canada (OPC). 2010b. *Privacy, Trust and Innovation – Building Canada's Digital Advantage*. Submission from the Office of the

Privacy Commissioner of Canada to the Digital Economy Consultation. 9 July. Ottawa: Office of the Privacy Commissioner.

Office of the Privacy Commissioner of Canada (OPC). 2010c. Notice of Consultation and Call for Submissions Privacy Implications of Cloud Computing. http://www.priv.gc.ca/resource/consultations/notice-avis_02_e.cfm. Retrieved April 2, 2011.

Office of the Privacy Commissioner of Canada (OPC). 2009. *Social Network Site Privacy: A Comparative Analysis of Six Sites*. February. Ottawa: Office of the Privacy Commissioner.

Office of the Privacy Commissioner of Canada (OPC). 2009a. *Deep Packet Inspection: A Collection of Essays from Industry Experts*. Ottawa: Office of the Privacy Commissioner. http://dpi.priv.gc.ca/. Retrieved April 2, 2011.

Office of the Privacy Commissioner of Canada (OPC). 2008. *Meeting of Two Worlds: the Legal and Information Technology (IT) Universes – Online Identity: Between Privacy and Virtual Profiles*. February. Ottawa: Office of the Privacy Commissioner.

Papacharissi, Zizi. 2010. Privacy as a Luxury Commodity. *First Monday* 15, no. 8 (2 August): http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3075/2581. Retrieved April 2, 2011.

Personal Information Protection and Electronic Documents Act (*PIPEDA*). 2000. http://www.privcom.gc.ca/legislation/02_06_01_e.asp. Retrieved April 2, 2011.

Public Interest Advocacy Centre (PIAC). 2009. *A "Do Not Track List" for Canada?* Ottawa: Public Interest Advocacy Centre. http://www.piac.ca/files/dntl_final_website.pdf. Retrieved April 2, 2011. Retrieved April 2, 2011.

Public Interest Advocacy Centre (PIAC). 2008. *All in the Data Family: Children's Privacy Online*. Ottawa: Public Interest Advocacy Centre. http://www.piac.ca/files/children_final_small_fixed.pdf. Retrieved April 2, 2011.

Public Interest Advocacy Centre (PIAC). 2004. *Consumer Privacy Under PIPEDA: How Are We Doing?* Ottawa: Public Interest Advocacy Centre. http://www.piac.ca/files/pipedareviewfinal.pdf. Retrieved April 2, 2011.

Raboy, Marc, and Jeremy Shtern. 2010. *Media Divides: Communication Rights and the Right to Communicate in Canada.* Vancouver: UBC Press.

Sagi, Douglas. 1970. Government May Regulate Computer Information Because Systems Pose Threat to Privacy. *The Globe and Mail*. 2 June, B7.

Shade, Leslie Regan. 2008. Reconsidering the Right to Privacy in Canada. *Bulletin of Science, Technology & Society* 28, no. 1 (February): 80-91.

Smythe, Dallas W. (2006). On the Audience Commodity and its Work (1981). In *Media and Cultural Studies Key Works*, eds. M.G. Durham and D.M. Kellner, 230-256. Malden, MA: Blackwell.

Stallworth, Brian. 2010. Future Imperfect: Googling for Principles in Online Behavioural Advertising. *Federal Communications Law Journal* 62, no. 2 (March): 465-491.

Whitehead, Martha J., and Catherine A. Quinlan. 2002. Canada: An Information Literacy Case Study. White Paper prepared for UNESCO, the U.S. National Commission on Libraries and Information Science, and the National Forum on Information Literacy, for use at the Information Literacy Meeting of Experts, Prague, The Czech Republic (July): http://www.nclis.gov/libinter/infolitconf&meet/papers/quinlan-fullpaper.pdf. Retrieved April 2, 2011.