Canadian Journal of Law and Technology

Volume 12 | Number 2 Article 1

6-1-2014

Access of Evil? Legislating Online Youth Privacy in the Information Age

Agathon Fric

Access of Evil? Legislating Online Youth Privacy in the Information Age

Agathon Fric[*]

I. INTRODUCTION

It has become so common to hear youth advocates plead, "Won't somebody think of the children?" that the question is now often invoked derisively. The question connotes children's powerlessness in making decisions that directly affect them, with the implication being that children are in need of protection from some new evil that threatens their innocence. Consider this: in October 2013, the second most-trafficked website on the Internet, Facebook.com, announced that opening its social network to users under the age of 13 is something it seriously considers.[1] Youth advocates balked at the mere suggestion that tweens — those between childhood and adolescence who are not yet teenagers — might be exposed to the privacy risks posed by sharing their personal information online. However, it is not just Facebook that raises the ire of privacy groups. In fact, a 2013 study by the Pew Research Center's Internet & American Life Project, jointly conducted with researchers at Harvard University's Berkman Center for Internet & Society, suggests that Facebook is losing clout among today's teens.[2] No longer considered as "cool" as it once was, hundreds of new mobile applications or "apps" targeting the under-18 demographic have emerged in its wake. For example, Snapchat is one of the fastest-growing apps among youth. The company's logo features a ghost, alluding to Snapchat's claim that photos posted by users on the service will automatically "disappear" after the intended recipients view the photos for one to ten seconds. Snapchat explains its philosophy in its *Guide for Parents*:

> On traditional social networks, users [. . .] feel pressure to curate the perfect representation of their lives for their friends . . . It's normal to worry about what people in your network might think about the things that you post. Sometimes this means that we say things that we think people will like, rather than expressing who we really are.

---

[*] Agathon Fric is a Juris Doctor candidate at Dalhousie University's Schulich School of Law and holds a Bachelor of Arts (Honours) in Political Science from Carleton University. He wishes to thank Professor Elizabeth Hughes for introducing him to privacy law as it relates to youth, for her infectious enthusiasm, and for her endless encouragement. Agathon's essay, here reproduced, is the 2014 winner of the IT.Can Student Writing Contest, a prize he accepted at the 18th Annual Canadian IT Law Association Conference in Montreal.

1 Anton Troianovski & Shayndi Raice, "Facebook Explores Giving Kids Access", *The Wall Street Journal* (4 June 2012) online: WSJ <http://online.wsj.com>.

2 Mary Madden et al, "Teens, Social Media, and Privacy" (Washington, DC: Pew Research Center, 2013) at 2, online: Pew Internet & American Life Project <http://www.pewinternet.org>.

> Snapchat creates a place to be funny, honest or however else you might feel when you take and share a snap with family and friends. *It's sharing that lives in the moment, and stays in the moment*.[3]

Yet, despite marketing itself as a place where youth can be honest without fear of repercussion, Snapchat's privacy policy tells a different, and more accurate, story:

> We cannot guarantee that deletion always occurs within a particular timeframe. We also cannot prevent others from making copies of your Snaps (e.g., by taking a screenshot). [. . .] In addition, as for any other digital information, there may be ways to access Snaps while still in temporary storage on recipients' devices or, forensically, even after they are deleted. *You should not use Snapchat to send messages if you want to be certain that the recipient cannot keep a copy*.[4]

The ghost is therefore an appropriate icon for Snapchat, not because the photos posted to it are actually ephemeral, but because the "Snaps" might never fade away and youth could be haunted by them for years to come. Saying one thing and doing another is not a new phenomenon; however, inducing youth to register for a website and surrender their personal information without knowing what they are getting into poses a problem.

The particular developmental challenges of youth make them vulnerable to privacy invasions online that capitalize on their credulity and commoditize their personal information in ways that are not always readily apparent and with potential consequences that are still less understood. The current legal regime in which private organizations collect, use, and disclose the personal information of Canadian youth for commercial purposes has advantages and disadvantages. However, proposals for reform have so far myopically focused on tinkering with the existing consent-based model of informational privacy, which ignores youth's own changing expectations of privacy. This suggests that in seeking to "protect" youth's privacy online, legislators have disempowered children and their parents from determining what information practices are acceptable for them. The law should instead respect these choices, while providing families with the tools necessary to exercise them.

(a) Method

This article seeks to address what constitutes youth online privacy, how youth conceive of their privacy, whether their privacy needs protecting, and, if so, how youth privacy should be regulated online. First, the article begins by rooting the issue of online youth privacy in the current social, technological, economic, political, and legal context, drawing on social science research to demonstrate both the threats and opportunities created by technology for youth privacy.

---

3 Snapchat, *Guide for Parents*, online: Snapchat <http://www.snapchat.com/static_files/parents.pdf> [emphasis added]. After this article was written, Snapchat tellingly revised the last line of its Guide for Parents on May 1, 2014 to read "It's sharing that lives in the moment, unless some one decides to save it."

4 Snapchat, *Privacy Policy*, online: Snapchat <http://www.snapchat.com/privacy> [emphasis added]. By the time of publication, Snapchat had replaced references to "Snaps" with the broader, seemingly innocuous term "messages."

Second, the analysis focuses on the relative strengths and weaknesses of current federal legislation as the primary law governing the collection, use, and disclosure of youth's personal information through their online activities, including their use of social networks and mobile applications or "apps." Under the *Constitution Act, 1867*, privacy is not explicitly assigned to the provinces or the federal government. Depending on the context, privacy may affect provincial domain over property and civil rights, or the federal power over trade and commerce. However, aside from British Columbia, Alberta, and Quebec, which have passed "substantially similar" legislation to the federal government, the federal statute applies to all private organizations across the country that collect information in the course of a commercial activity, even if they only carry on business in a single province.[5] Practically speaking, to the extent commercial websites collect young people's information across interprovincial or international borders, they are going to be governed by the federal statute, in recognition of the federal government's power to regulate interprovincial and international trade.[6] It is worth noting that Canadian jurisprudence on youth privacy online is underdeveloped by virtue of the fact that the Office of the Privacy Commissioner of Canada (OPC) generally diverts such grievances from the judicial system. Even then, the Privacy Commissioner has so far only conducted one investigation into a website that specifically targets youth.[7] Accordingly, the Commissioner's report into the complaint against Nexopia.com, a Canadian-made social network, figures prominently in this analysis. It serves as a case study of how federal privacy legislation is applied in practice, and an example by which the effectiveness of the existing regime may be evaluated.

Third, after canvassing the shortcomings of the current legal regime, I consider proposals for reform and assess their merits. This analysis draws on the legislative experience of the United States, both as a possible model for reform and as a cautionary tale. Given that many of the world's most popular websites among youth originate in the US, that country's Congress has arguably had a greater influence on the information practices and privacy policies affecting Canadian youth than any other. Finally, I offer an alternative legal solution to give more meaningful expression to youth privacy rights, while avoiding the paradigmatic trap of most existing proposals.

(b) Scope

Privacy law is a growing area of study. The sheer novelty of the Internet and new means of invading privacy ensure that the timeworn construction of law as an inherently reactive force will persist for some time to come. While this article is

---

5 Barbara McIsaac, Rich Shields & Kris Klein, *The Law of Privacy in Canada*, loose-leaf (Scarborough, Ont: Carswell), ch 1 at 17.

6 Office of the Privacy Commissioner of Canada, *Your Privacy Responsibilities: A Guide for Businesses and Organizations* (February 2010) at 3, online: OPC <http://www.priv.gc.ca/information/guide_e.pdf> [OPC, *Guide for Businesses*].

7 Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2012-001, "Social networking site for youth, Nexopia, breached Canadian privacy law" (29 February 2012) Introduction at para 11, online: OPC <http://www.priv.gc.ca> [OPC, "Nexopia"].

about youth privacy on the Internet, it is beyond the scope of the present analysis to delve into all the ways in which the World Wide Web threatens the privacy of youth. For instance, unsolicited or inadvertent access to pornographic and other mature content may constitute an intrusion upon children's privacy online, but this type of privacy infringement is outside the current scope. By the same token, this article is not, strictly speaking, about cyberbullying or other instances where youth use technology to intentionally violate the privacy of other youth, although this too is an increasingly common by-product of the collection, use, or disclosure of personal information by organizations when youth do not fully appreciate the potential consequences of sharing their information online.[8] Nor is this article about the collection, use, and disclosure of personal information by governments or public agencies, which are governed under a separate statutory regime.[9] This article focuses on youth privacy online from the perspective of privacy as information control. More specifically, it is concerned with the information management practices of private websites that collect, use, or disclose youth's personal information for profit, as regulated by the *Personal Information Protection and Electronic Documents Act*.[10] It is also about the reasonable or unreasonable privacy expectations that modern youth have over the information they share.

II. PRIVACY, THE INTERNET, AND YOUTH IN CONTEXT

Before evaluating the current legal environment in which Canadian youth find their privacy protected or unprotected, as the case may be, it would be prudent to describe briefly what is meant by privacy and to situate online privacy in the social, economic, and legal context in which youth find themselves. Broadly speaking, *privacy* describes the relationship between one's self and others. What is "private" is usually understood in contrast to what is "public." Thus, information is central to society's modern understanding of privacy.[11] Information about an individual — whether that be his or her name, age, birthdate, location, phone number, gender, race, Social Insurance Number, reputation, or favourite band — is no longer considered by many to be "private" if it becomes publicly available. At the same time, sharing information with others, in itself, does not necessarily correlate with diminished privacy. Depending on who has access to the personal information and what purposes they use it for, the information may remain private as between the two, or three, or however many parties with which it is shared. In this sense, an *invasion* of privacy occurs when one of the parties privy to the information collects, uses, or discloses some or all of it for a purpose or in a manner with which the individual

---

8 For a comprehensive treatment of cyberbullying as a social phenomenon and its interplay with the law, see Shaheen Shariff, *Cyber-bullying: Issues and solutions for the school, the classroom, and the home* (London: Routledge, 2008).

9 See *Privacy Act*, RSC 1985, c P-21.

10 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].

11 Bernard Richard, "There Ought To Be A Law: Protecting Children's Online Privacy in the 21st Century" (Paper delivered by the Working Group of Canadian Privacy Commissioners and Child Youth Advocates, 19 November 2009) at 5, online: Government of New Brunswick <http://www.gnb.ca/0073/PDF/Children'sOnlinePrivacy-e.pdf>.

whom the information is *about* did not agree. In other words, privacy is breached when one loses *control* over his or her own information.[12] Therefore, privacy is best understood as a spectrum: how much privacy one has, and over what pieces of information, depends on the extent to which the individual retains control over his or her information.

(a) Society and Technology

The aggressive collection, use, and disclosure of young people's information on the Internet did not begin with the advent of social networks such as MySpace, Facebook, and Twitter, but the proliferation of these websites has intensified concerns among parents and privacy groups about the consequences of sharing mounds of data over time. The information that these sites collect is highly sensitive. For example, in 2013 researchers developed a model that accurately predicts the sexual orientation of Facebook users in 88% of cases, and can differentiate between Caucasians and Blacks 95% of the time, using only a user's Facebook "Likes," which are used to express a "positive association" with a particular brand, artist, public figure, or social issue.[13] Such tools could lead to serious invasions of privacy using seemingly benign preferences that are publicly available by default. Few things are as intensely personal and private as one's sexual orientation. This demonstrates that youth privacy online is not merely jeopardized by the information that youth *think* they are sharing explicitly, but also by what can be *inferred* from their public disclosures. Such technology would make it easy for employers to stereotype job applicants and discriminate against them based on the information that they have shared online. The fear, then, is that youth are not capable of judging the potential consequences of their actions online. On the other hand, the study also reveals a unique opportunity: social scientists can conduct more meaningful research using wider data sets than ever before, making their findings more reliable and potentially more relevant.

Youth privacy exists in a social context where children and teens feel pressured to participate in online forums. As one teenager put it, "If you're not on MySpace, you don't exist."[14] A young person's social network of choice may vary, but the sentiment is the same. In this way, those youth who would rather not share their information online due to personal reasons — or because they actually appreciate the harm that can come from unauthorized intrusions into their privacy — risk being ostracized by their peers if they withdraw from the online sphere. Thus, peer pressure reinforces and normalizes the collection, use, and disclosure of youth's personal information by commercial websites that offer youth these social spaces.

---

12 *Ibid.*

13 Michal Kosinski, David Stillwell & Thore Graepel, "Private Traits and Attributes Are Predictable From Digital Records of Human Behaviour", online: (2013) 110:15 Proceedings Nat'l Academy Sci Early Ed 5802 <http://www.pnas.org>.

14 Danah Boyd & Alice E Marwick, "Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies" (Paper delivered at the Oxford Internet Institute, A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, 22 September 2011) at 8, online: SSRN <http://www.ssrn.com/abstract=1925128>.

Youth also have a selfish reason for sharing personal information about themselves with commercial websites. Privacy and especially one's control over personal information is central to one's self-image. In choosing what information to selectively disclose, youth are able to shape both how they see themselves and how others perceive them. In this sense, curating an online profile that discloses one's likes and dislikes, opinions, or beliefs is akin to changing hairstyles or wearing new outfits. Focus groups have shown that youth release personal information online to assert independence from parents, to interact with friends, and to experiment with new identities.[15] During adolescence, youth are still in the process of forming their identities as young adults. The Internet makes it possible for youth to test different ideas and presentations of themselves without the same commitment that would be required of, for example, getting a tattoo to express the same. They can alter their image simply by disclosing more or less, or different types of, information.

As a result, youth's liberal disclosure of information on social networks has led some to believe that teens do not care about their privacy. This is not true.[16] However, it is true that parents are far more concerned than their children about the effect that sharing information online has on their children's privacy. In 2012, just 9% of American teens said they were "very concerned" and 31% were "somewhat concerned" about their information being shared online or used by third party advertisers. By contrast, 81% of parents said they were "very" or "somewhat concerned."[17] It is fair to assume a similar trend exists in Canada, where 99% of children use the Internet regularly and 94% of youths' top 50 favourite websites collected information from them in 2007.[18] That parents are more concerned is not surprising. After all, it is a parent's job to take care of his or her children and to look out for their best interests. However, their concern is rooted in the particular characteristics of modern Internet technologies. Information that private websites collect can be aggregated, manipulated, repackaged, and resold more quickly and more cheaply than ever before. Furthermore, information that youth post online is characterized by its permanence and a potentially limitless audience.[19]

On the other hand, while youth feel pressure from friends to share personal information online, society also has a general interest in surveillance. Historically, society has been sceptical of people who claim a right to privacy. After all, if one has nothing to hide, why would he or she need privacy? At the same time that parents lament what they perceive to be their child's loss of privacy online, they are

---

15 Valerie Steeves, Trevor Milford & Ashley Butts, *Summary of Research on Youth Online Privacy* (Ottawa: Office of the Privacy Commissioner of Canada, 28 March 2010) at 15.

16 House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Privacy and Social Media in the Age of Big Data* (April 2013) at 22–30 (Chair: Pierre-Luc Dusseault) at 24.

17 Madden et al, *supra* note 2 at 10.

18 Jacquelyn Burkell, Anca Micheti & Valerie Steeves, "Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand" (March 2007) at 9, online: On the Identity Trail <http://www.idtrail.org/files/broken_doors_final_report.pdf>.

19 Shariff, *supra* note 8 at 33.

often quick to rely on their child's Internet activities as a means of surveillance.[20] In this way, parents are complicit in violating their own child's sense of privacy. The collection, use, and disclosure of children's personal information becomes both a blessing and a curse, creating a disincentive for parents to discourage children from sharing personal information online. Of course, this is not true of all parents or those who are more trusting of their children, but stories of parents snooping in their children's rooms are not unusual. Online surveillance for socializing with friends has the indirect effect of making it easier for parents to pry. Therefore, there are strong pressures for society to collect and for youth to share personal information, facilitated by new Internet technologies.

(b) Economy and Politics

The economic incentives to undermine youth privacy through the online collection, use, and disclosure of children and teen's personal information are tremendous. In Canada, youth aged 9 to 14 spend over $1.9 billion annually and influence another $20 billion in family purchases.[21] Those numbers balloon when you add the market power of teenagers between 15 and 17. Since children do not have the same financial obligations as adults, this is almost entirely discretionary spending that is up for grabs. With youth spending more and more time online and revealing more personal information than ever before, advertisers have developed sophisticated new ways to target youth. For example, through the use of *online behavioural advertising* third parties can track a user's activities online, including what links a user clicks, what strings a user searches, and what products a user purchases.[22] Taken together, this information enables advertisers to create a profile on a particular user's preferences, which can then be used to display ads specifically tailored to the unique user. By only advertising a particular product or service to users that have a proven disposition toward that subject, online behavioural advertising is a more effective marketing vehicle than traditional advertising, where dollars are wasted on a mass of people who may never be interested in the thing being promoted. Collecting youth's information to target customers promises that businesses will save money on advertising, sell more product, and increase the relevance of advertising shown to youth.

A recent example illustrates the attractiveness of this model to big business. In November 2013, Facebook offered to buy Snapchat for $3 billion USD, despite the fact that Snapchat has never generated a penny of revenue.[23] What Snapchat lacks in profit, it more than makes up for with personal information, which buyers see as a resource that has yet to be exploited. It is thus not surprising that Snapchat's CEO

---

20 Boyd & Marwick, *supra* note 14 at 5.

21 Valerie Steeves, "It's Not Child's Play: The Online Invasion of Children's Privacy" (2006) 3:1 U Ottawa L & Tech J 169 at 174.

22 House of Commons, *supra* note 16 at 3.

23 Evelyn M Rusli & Douglas MacMillan, "Snapchat Spurned $3 Billion Acquisition Offer from Facebook", *The Wall Street Journal* (13 November 2013) online: WSJ <http://online.wsj.com>. By August 2014, Snapchat's value had more than tripled: Evelyn M Rusli & Douglas MacMillan, "Snapchat Fetches $10 Billion Valuation", The Wall Street Journal (26 August 2014) online: WSJ <http://online.wsj.com>.

rejected Facebook's offer, betting on an opportunity to parlay the information that the app has collected on its users into targeted advertising revenue and in-app purchases. The problem with this kind of advertising, however, is that it encourages companies to collect information of youth deceptively. It depends on the acquiescence of youth who do not know any better and employs surreptitious techniques that avoid drawing attention to their operation. A 2012 study by the US, Federal Trade Commission discovered that only one in five mobile apps that target kids to collect their personal information actually posts a privacy policy.[24] Some websites targeted to youth, like Neopets.com, create immersive online environments that embed advertising directly into the website's games, blurring the line between content and advertising.[25] Others use vague or technical language[26] to avoid explaining to users what is actually quite simple: companies follow them, and they do so primarily for their own economic benefit. Without the user's explicit consent, companies effectively deprive the individual of the choice as to whether the benefit of receiving more relevant advertising is worth the price to his or her privacy.

Facebook CEO Mark Zuckerberg has tried to argue that people no longer have a reasonable expectation of privacy.[27] To be fair, what Zuckerberg probably means is that the world's embrace of social networks like Facebook reflect a broader change in people's attitudes toward privacy, rather than suggesting that any expectation of privacy was obliterated by Facebook's arrival. Either way, Zuckerberg's opinion only serves to justify his own economic interest in the unfettered access to user data to generate revenue. Again, it attempts to suppress a dialogue with users as to what their reasonable expectations are and substitutes the answer that "Big Business" wants.

The economic imperative for companies to collect personal information is also a political one. In the 1990s, the federal government set out on what was arguably the largest nation-building exercise since the transcontinental railway and, by the new millennium, every public school in Canada was connected to the web.[28] While this has had knock-on effects, such as enhancing learning, one of the main drivers cited for the government initiative was to ensure that Canada remains "competitive in the . . . information marketplace."[29] Similarly, the purpose of the federal statute governing commercial organizations' collection, use, and disclosure of personal information is:

> . . . to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the

---

24 US, Federal Trade Commission, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (Washington, DC: FTC, December 2012) at 6.

25 John Lawford, *All in the Data Family: Children's Privacy Online* (Ottawa: Public Interest Advocacy Centre, 2008) at 24, online: PIAC <http://www.piac.ca>.

26 Burkell, Micheti & Steeves, *supra* note 18 at 18.

27 Bobbie Johnson, "Privacy no longer a social norm, says Facebook founder", *The Guardian* (11 January 2010) online: Guardian Unlimited <http://www.guardian.co.uk>.

28 Burkell, Micheti & Steeves, *supra* note 18 at 9.

29 Steeves, *supra* note 21 at 171.

> need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[30]

The primary legislation governing youth privacy online in Canada thus has a dual purpose, which reflects the government's interest in economic growth, and presumably a larger tax base, at the expense of individual privacy over personal information. Hence, lawmakers and businesspeople alike have a vested interest in collecting the information of Canadian youth.

(c) Law and History

The law has historically recognized the unique vulnerabilities of youth and their right to be protected from exploitation. For instance, in the 1989 decision of the Supreme Court of Canada in *Irwin Toy Ltd. v. Quebec (Attorney General)*,[31] a majority of the court upheld Quebec's prohibitions on advertising to children under the age of 13 as a reasonable limit on advertisers' freedom of speech under section 2(b) of the *Canadian Charter of Rights and Freedoms*. In their reasons, the majority held:

> . . . the concerns which have motivated both legislative and voluntary regulation in this area are the particular susceptibility of young children to media manipulation, their inability to differentiate between reality and fiction and to grasp the persuasive intention behind the message . . .[32]

The decision reflects the court's willingness to treat all children under 13 as a single class, despite the fact that some may be more vulnerable to manipulation than others. More recently, Justice Abella echoed this preference for treating children as a vulnerable class in society in *A.B. (Litigation Guardian of) v. Bragg Communications Inc.*[33] Although that case primarily centred on when a party to a civil proceeding may proceed anonymously, it also addressed the issue of whether or not a child victim of cyberbullying had to prove that she personally suffered harm before a court can order a publication ban on the contents of a fake Facebook profile. Abella J., writing for a unanimous bench, said:

> Recognition of the inherent vulnerability of children has consistent and deep roots in Canadian law. [. . .] As a result, in an application involving sexualized cyberbullying, there is no need for a particular child to demonstrate that she personally conforms to this legal paradigm. The law attributes the heightened vulnerability based on chronology, not temperament.[34]

In other words, a youth's age dictates the extent to which the law will treat him as vulnerable. This, in turn, may affect the way law regards the reasonableness of the

---

30 *PIPEDA*, *supra* note 10, s 3.

31 *Irwin Toy Ltd. v. Quebec (Attorney General)*, 1989 CarswellQue 115F, 1989 CarswellQue 115, [1989] 1 S.C.R. 927, 58 D.L.R. (4th) 577 (S.C.C.) [*Irwin Toy*].

32 *Ibid* at para 72.

33 *A.B. (Litigation Guardian of) v. Bragg Communications Inc.*, 2012 SCC 46, [2012] 2 S.C.R. 567, 2012 CarswellNS 676, 2012 CarswellNS 675 (S.C.C.) [*Bragg*].

34 *Ibid* at para 17.

collection, use, and disclosure of youth's personal information by commercial organizations.

A similar approach is routinely applied in criminal law, where the *Criminal Code* draws bright lines of liability based on age. Section 13 shields children aged 11 and under from criminal liability either because they are believed to be incapable of forming the requisite *mens rea* to be convicted, or because society has decided through its elected representatives that the criminal law is not the appropriate tool to discipline kids behaving badly.[35] Meanwhile, youth aged 12 to 17 may be charged criminally, but their relative immaturity compared to adults is still recognized by the fact that they fall under the *Youth Criminal Justice Act*'s separate statutory scheme, which emphasizes rehabilitation over incarceration.[36] The *YCJA* also protects youth privacy by preventing media from publishing the names of youth criminals. These provisions reflect the legislature's intention to diminish the moral responsibility attached to young offenders based on generalizations about youth of a particular age, rather than a youth's particular capacity.

However, notwithstanding the law's tendency to sometimes group children into one or more classes based on age, other areas of law take into account the specific faculties of an individual youth. For instance, in tort law Canadian courts have adopted a modified test for determining a child's liability in negligence when they are above tender age, but below full maturity. The child's standard of care is not what any reasonable child of a particular age would do, but what a reasonable child of like age, intelligence, and experience would have been expected to do in the circumstances.[37] The law of negligence thus considers the unique capacity of children on a case-by-case basis. Likewise, in health law, the doctrine of the mature minor declines to lump all minors into a single category based on age. Instead, it suggests that minors who can demonstrate sufficient maturity to understand the consequences of consenting to or refusing treatment should have their wishes respected.[38] Here, as with negligence, the law factors the youth's individual capacity into its analysis, rather than applying general assumptions based on age to young people as a group. It is within this context — in which the law has opted to treat all youth in the same way for some purposes and as unique individuals for other purposes — that approaches to regulating the collection, use, and disclosure of youth's personal information online can be understood.

A court's assessment of youth as a vulnerable class may also be interpreted through the lens of international law. Article 16 of the United Nations *Convention on the Rights of the Child* recognizes the right to privacy of children under 18 as a human right. However, this right should be construed in light of a child's right to free expression "through any . . . media of the child's choice" in Article 13 and Article 17's recognition of the important role media plays in ensuring youth can

---

35 *Criminal Code*, RSC 1985, c C-46, s 13.

36 *Youth Criminal Justice Act*, SC 2002, c 1, s 3 [*YCJA*].

37 Gerald HL Fridman, *The Law of Torts in Canada*, 3d ed (Toronto: Carswell, 2010) at 465.

38 *Manitoba (Director of Child & Family Services) v. C. (A.)*, 2009 CarswellMan 294, 2009 CarswellMan 293, 2009 SCC 30, [2009] 2 S.C.R. 181 (S.C.C.) at para 87 [*AC*].

access a diverse range of perspectives.[39] In this sense, these provisions support legislation that protects children's privacy, while appreciating that such protection should not come at the expense of a child's choice to express himself through online media that adults believe will undermine youth privacy. From this human rights perspective, regulating the collection, use, and disclosure of information does not serve an instrumental purpose to protect youth *as consumers*. Rather, it recognizes that privacy is inherently worthy of protection for its own sake, balanced against a youth's legitimate interest in free expression. Ultimately, online behavioural advertising and other covert uses of youth's personal information betray a young person's autonomy and human dignity. Thus, there is little debate that youth privacy needs to be safeguarded in the Internet age. The question is *how* youth privacy should be regulated and whether the legislative regime currently in place is effective.

III. PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)[40] is the centrepiece of the federal government's private-sector privacy regulation. It purports to protect the personal information of all Canadians, including youth, against commercial website operators, among others. The statute has advantages and disadvantages. On one hand, the law covers a broad spectrum of personal information. It is flexible enough to take account of the impressionability of youth and to tailor privacy protections to their particular needs as a class. The law also promotes transparency in how information is used and respects individual autonomy by requiring informed consent to the collection, use, and disclosure of personal information. However, the Privacy Commissioner's interpretation and administration of the *Act* raises significant concerns about the adequacy of existing privacy protections for youth online. It is useful to briefly summarize the scheme of the *Act* before assessing its strengths and weaknesses.

(a) Statutory Scheme

Although it was enacted in 2000, *PIPEDA* did not start to govern the collection, use, and disclosure of personal information by all private organizations in the course of a commercial transaction, including websites, until 2004.[41] Since then, companies that engage in any of these information practices must comply with the provisions of the *Act*. Specifically, section 5(1) requires organizations to obey ten principles contained in Schedule 1, which constitute national standards for handling personal information. Of particular relevance to youth privacy are Identifying Purposes, Consent, Limiting Use, and Openness (principles 4.2, 4.3, 4.5, and 4.8, re-

---

39 *Convention on the Rights of the Child*, 20 November 1989, 1577 UNTS 3, Can TS 1992 No 3 (entered into force 2 September 1990), online: United Nations Treaty Collection <http://untreaty.un.org>.

40 *PIPEDA*, *supra* note 10.

41 OPC *Guide for Businesses*, *supra* note 6 at 3.

spectively).[42] These principles intersect and overlap. In substance, they require websites collecting, using, or disclosing personal information about their users or any other site's users to explicitly identify the purposes for which the information will be collected, used, or disclosed and to obtain the user's knowledge and meaningful consent to gather the information for those purposes. Related to this end, principle 4.3.2 requires organizations to take "reasonable efforts" to inform the individual of the purposes to which his information will be put and to state the purposes in a manner such that the user can "reasonably understand" how the information will be used.[43] Once consent has been obtained, the organization may only use the information for those stated purposes. If the organization wishes to use the information for a new purpose, it must seek the user's renewed consent.[44] Under principle 4.3.6, consent may be express or implied, but implied consent should generally be reserved for information of a less sensitive nature. Otherwise, there is no specific requirement for what form consent must take.[45]

The collection, use, or disclosure of information *beyond* what is required to fulfil the explicit purpose cannot be a condition of using the website.[46] This rule discourages sites from collecting more information than necessary. Sites are not precluded from collecting more information than necessary, but under this principle users should be allowed to opt out of such practices and still be able to use the website. Furthermore, section 5(3) of *PIPEDA* contains an overriding reasonableness requirement. It states that organizations can "collect, use, or disclose personal information only for purposes that a reasonable person would consider [. . .] appropriate in the circumstances." This means that certain collections, uses, or disclosures of personal information will be against the law, notwithstanding whether or not an individual user gives consent. Lastly, *PIPEDA* applies to all Canadians, regardless of age. It makes no special provision for youth privacy online.

The *Act* is administered by the Privacy Commissioner of Canada who, as an independent officer of Parliament, reports to the House of Commons and the Senate.[47] The current Commissioner, Daniel Therrien, is responsible for promoting privacy rights and investigating complaints made under section 11 of *PIPEDA*. He can also launch an investigation on his own initiative. The Commissioner issues a report on his findings and makes recommendations to resolve violations of the *Act*.[48] If the organization does not comply, section 14 empowers the Commissioner to take action in Federal Court, although matters are generally resolved before reaching this stage.

---

42 *PIPEDA*, *supra* note 10, Schedule 1.

43 *Ibid*, Schedule 1, s 4.3.2.

44 *Ibid*, Schedule 1, s 4.2.4.

45 *Ibid*, Schedule 1, s 4.3.7.

46 *Ibid*, Schedule 1, s 4.3.3.

47 Office of the Privacy Commissioner of Canada, *About the Office of the Privacy Commissioner*, online: OPC <http://www.priv.gc.ca>.

48 *PIPEDA*, *supra* note 10, s 13.

(b) Strengths

One of *PIPEDA*'s greatest strengths in terms of its ability to protect youth privacy online is that it covers a broad range of personal information. The *Act* defines "personal information" as any "information about an identifiable individual . . ."[49] This includes not only information that immediately identifies an individual, like one's name, address, or Social Insurance Number, but also age, race, religion, height, weight, marital status, education, email address, IP address, and purchase history.[50] The definition is so wide that it would cover Facebook likes and general preferences, whether they are tied to a particular person's name or not. This means youth who adopt an alternate identity online could still be assured that their personal information is governed by fair information principles. This is important because what is or is not "identifying" information is a matter of degree rather than kind. If enough pieces of information are collected about an individual's preferences, they can be used to create a profile of the person who released them, which may, in turn, be traced back to the individual. Thus, *PIPEDA*'s definition supports youth privacy by including virtually all of their information within its scope.

Meanwhile, the statute takes a pragmatic approach to youth privacy online by accommodating youths' credulity. Although *PIPEDA* does not explicitly compel organizations to treat minors' personal information differently than that of adults, the requirement in section 5(3) that personal information may only be collected, used, or disclosed for purposes that a reasonable person would consider appropriate is sufficiently flexible to hold websites that collect information from *youth* to a higher privacy standard than those that do not. For example, in 2012 the Public Interest Advocacy Centre filed a complaint against the youth-oriented social network Nexopia.com on the basis that a reasonable person would not consider its information practices appropriate vis-à-vis youth. Following an investigation, the Privacy Commissioner at the time, Jennifer Stoddart, agreed with the complainant. In particular, the Commissioner said that whenever children's information is involved, what is considered "reasonable" under section 5(3) would change. As a result, Nexopia's practice of making all users' profile information publicly available to anyone on the Internet by default was unreasonable.[51] The Commissioner's finding is significant because she could have easily found that the practice was inappropriate because young users did not *know* about the default setting and, consequently, could not meet the "knowledge and consent" requirement of principle 4.3. This was arguably the case, as the Commissioner held that Nexopia's privacy policy did not explicitly state the fact that it shared users' information publicly by default.[52] However, the Commissioner went further, finding that the practice was inappropriate for young people *by virtue of their youth*. Assuming users were informed of the public setting and meaningfully consented to this use of their information, the Commissioner's decision suggests that children are nevertheless in need of protection from future harm that may come from publicly revealing this

---

49 *Ibid*, s 2(1).

50 Office of the Privacy Commissioner of Canada, Interpretation Bulletin, "The Meaning of 'Personal Information'" (2 October 2013).

51 OPC, "Nexopia", *supra* note 7, Section 1 at paras 92–95, 107.

52 *Ibid*, Section 1 at para 108.

information online. The case may be confined to its facts, since the Commissioner found that the information Nexopia disclosed was highly sensitive data, including youths' drug use and sexual activity;[53] however, it is not uncommon for youth to share this kind of personal information online. This signals that the Privacy Commissioner will interpret section 5(3) as requiring substantively different safeguards for youth as a class based on age, even though the statute does not distinguish explicitly between the privacy needs of adults and youth.

In cases where a reasonable person *would* consider the collection, use, or disclosure of a youth's personal information appropriate, *PIPEDA* may still hold websites to a higher standard in dealing with youth. Commenting on the need for "meaningful consent," the Privacy Commissioner's official policy on Online Behavioural Advertising states: "What is meaningful for a 17-year-old may not be the same as what is meaningful for a 9-year-old. Practices need to correspond to cognitive and emotional development. What is appropriate will also depend on the specific context."[54] At least in theory, this suggests that websites collecting youths' personal information will need to show that they took reasonable steps to inform their young users about their data use practices in a way that youth can understand.

Moreover, *PIPEDA*'s positive requirement that organizations only use information for the explicit purposes for which the information is collected promotes transparency. Youth are less likely to feel that their privacy has been violated if they are made fully aware of how and why their personal information is being used in terms that are cognizable to them. This improves the likelihood that youth can form the requisite consent to the collection and use of their personal information, enabling them to make a conscious choice as to whether or not the perceived benefit from using the website is worth the privacy trade-off. In addition, the simple fact that *PIPEDA* requires organizations to obtain consent from the individuals whose personal information they seek, as opposed to letting advertisers have free rein to gather information without notice, enshrines respect for individual autonomy, which is central to youths' privacy and their dignity as human beings.[55] Therefore, *PIPEDA*'s provisions respond to many of the concerns about youth privacy online, by creating room to adapt its protections to account for young people's unique vulnerabilities.

(c) Weaknesses

Notwithstanding the advantages of having a statute with flexibility, *PIPEDA* creates too much wiggle room for websites collecting youths' personal information for it to effectively defend youth privacy online. Firstly, the Office of the Privacy Commissioner's application of the law contradicts its own policy positions. In its policy on Online Behavioural Advertising from June 2012, the Commissioner advises that websites should avoid tracking children altogether as a best practice because "The key issue here is the great difficulty organizations are likely to encounter in obtaining meaningful consent to OBA from very young users of the

53 *Ibid*, Section 1 at paras 17–18.

54 Office of the Privacy Commissioner of Canada, *Policy Position on Online Behavioural Advertising* (June 2012), online: OPC <http://www.priv.gc.ca> [OPC, *OBA Policy*].

55 House of Commons, *supra* note 16 at 61.

Internet."[56] In spite of the Commissioner's suggestion that the reasonableness of an information practice under section 5(3) is qualitatively different when children are involved (particularly as it relates to public-by-default settings), the Commissioner apparently draws the line when it comes to online behavioural advertising. Paradoxically, even though the OPC suspects youth could not meaningfully consent to such practices given their complexity, the Commissioner has adopted the position that tracking users' Internet traffic across the web *can* be an appropriate purpose for collecting, using, and disclosing personal information so long as it is not required as a condition of service.[57] Thus, in the Nexopia investigation, the Privacy Commissioner did not recommend that Nexopia stop tracking children, but simply suggested the site should allow them to opt out, which is the same standard that the Privacy Commissioner applies to the tracking of adults.[58] Considering the stealth of tracking technologies that often deprive users of a conscious choice to share information about their surfing habits and the Commissioner's own admission that youth will have difficulty in consenting to these practices, it is puzzling how the Commissioner can argue that the reasonableness of using such techniques is unchanged in the context of youth. The result is an unprincipled patchwork of interpretation that fails to meaningfully protect youth privacy. It demonstrates *PIPEDA*'s inability to give clear notice to website operators as to what uses of youths' personal information will or will not be acceptable.

Secondly, underpinning *PIPEDA*'s incoherent privacy protections are the statute's conflicting purposes. The Federal Court of Appeal considered the *Act*'s interpretation in *Englander v. Telus Communications Inc.*[59] in which the applicant argued it was unreasonable for Telus to require a customer's consent to publish his information in the company's white pages and to charge a $2.00 service fee if the customer later wanted his number unlisted. The court found that this was a reasonable purpose within the meaning of section 5(3), but that Telus had to be more explicit in notifying customers that their numbers would be published. In contrasting the goals of the public sector's *Privacy Act* with the private sector's *PIPEDA*, the court held:

> The purpose of [*PIPEDA*] is altogether different. It is undoubtedly directed at the protection of . . . privacy; but it is also directed at the collection, use and disclosure of personal information by commercial organizations. It seeks to ensure that such collection, use and disclosure are made in a manner that reconciles, to the best possible extent, an individual's privacy with the needs of the organization. There are, therefore, two competing interests within the purpose of the [*PIPEDA*]: an individual's right to privacy on the one hand, and the commercial need for access to personal information on the other. However, there is also an express recognition, by the use of the

---

56 OPC, *OBA Policy*, *supra* note 54.

57 *Ibid.*

58 OPC, "Nexopia", *supra* note 7, Section 3 at paras 59–62.

59 *Englander v. Telus Communications Inc.*, 2004 CarswellNat 5422, 2004 FCA 387, [2005] 2 F.C.R. 572, 2004 CarswellNat 4119 (F.C.A.).

> words "reasonable purpose," "appropriate" and "in the circumstances" (repeated in subsection 5(3)), that the right of privacy is not absolute.[60]

In this sense, privacy, far less youth privacy, is not the only or even the main factor that courts will consider in assessing whether information practices are appropriate. The Privacy Commissioner adopted a similar stance in a 2009 report responding to a complaint against Facebook, in which it conceded that since nothing is free and websites have to pay for the costs of offering their services, collecting users' information to generate advertising revenue is a reasonable condition of using their sites under section 5(3).[61] This may explain why the Privacy Commissioner thinks it is reasonable for youth to consent to online behavioural advertising (notwithstanding the inherent challenge of actually obtaining true consent), and unreasonable for youth to consent to the open disclosure of their information to the public by default. In one case, the practice makes profit. In the other, there is no obvious financial benefit. As a result, *PIPEDA*'s privacy safeguards amount to half-measures. They operate within a scheme in which privacy is not worthy of protection for its own sake, but rather privacy is something that must be "reconciled" to the instrumental objective of economic necessity. Although no right is absolute, the *Act* as presently constituted uses privacy as a means to an end, rather than an end in itself. Consequently, its ability to meaningfully protect youth privacy is inhibited right out of the gate by conflicting purposes.

Unfortunately, it is not open to youth to challenge the adequacy of this legislation on the basis that it is not in a child's best interests; that is, assuming privacy is in a child's best interests. In *Canadian Foundation for Children, Youth & the Law v. Canada*, the Supreme Court of Canada found no consensus that laws should always be in the best interests of the child, so this could not be a principle of fundamental justice.[62] Accordingly, youth could not succeed in a section 7 *Charter* challenge to *PIPEDA* on the ground that the *Act*'s infringement of their privacy is not in their best interests. Assuming a deprivation of privacy engages section 7's liberty and security of the person protections, one must prove that the deprivation is also inconsistent with a principle of fundamental justice before a *Charter* violation is found.

Thirdly, the Privacy Commissioner's administration of *PIPEDA* in the Nexopia investigation may have unintended consequences. Nexopia had argued that, unlike Facebook, it was an "open" network where users did not merely seek to communicate with friends but to "show off" to the world. As such, the site's owners argued that increasing its default privacy settings would flout the reasonable expectations of its users.[63] The Privacy Commissioner did not accept that argu-

---

60 *Ibid* at para 38.

61 Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2009-008, "Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc" (16 July 2009) at para 131, online: OPC <http://www.priv.gc.ca>.

62 *Canadian Foundation for Children, Youth & the Law v. Canada (Attorney General)*, 2004 CarswellOnt 253, 2004 CarswellOnt 252, 2004 SCC 4, [2004] 1 S.C.R. 76 (S.C.C.) at para 10.

63 OPC, "Nexopia", *supra* note 7, Section 1 at paras 69–71.

ment, relying on Nexopia's privacy policy for evidence, which suggested the site had more to do with interacting with friends than the public. However, the Commissioner was not content to have Nexopia amend its privacy policy to clarify its public intentions, which would at least bring it in line with principle 4.3.2's requirement to obtain "knowledge and consent." She argued that because Nexopia targeted youth, it was inappropriate to share youths' personal information publicly by default under section 5(3).[64] This may well have a chilling effect on websites targeted toward youth. Although the result of the OPC's report is that youth can still post information publicly after specifically selecting that option, it creates an incentive for websites to adopt an "open" network infrastructure where everything is made public and no privacy options are available so as to avoid any accusation that its privacy practices are inconsistent with the reasonable expectations of its users. In this sense, Nexopia's mistake was that it provided optional privacy restrictions in the first place. If nothing is private, then there can be no confusion about what will or will not be shared publicly, which theoretically makes it easier for a website to satisfy the "knowledge and consent" requirement under the *Act*. This has negative repercussions for youth privacy online because youth will sign up for such "open" networks to express themselves, regardless of whatever the Privacy Commissioner thinks is an appropriate level of default privacy vis-à-vis youth. Thus, the Commissioner's interpretation of section 5(3) may actually undermine youth privacy by discouraging sites from implementing optional privacy controls.

Fourthly, *PIPEDA* does not safeguard against prospective harms that may be caused by collecting, using, or disclosing youth's personal information. In *Turner v. Telus Communications Inc.*,[65] the applicant challenged Telus' collection of its employees' voiceprints for internal network authentication. On appeal, the Federal Court of Appeal held that the collection was for a reasonable purpose within the meaning of section 5(3) of *PIPEDA*. In the course of its judgment, the court noted that a "reasonable" purpose is to be judged in light of current circumstances. By contrast, new technologies and uses for personal information are "to be tested only when they are real and meaningful, not when they are hypothetical."[66] One can appreciate the court's desire to judge the reasonableness of collecting, using, and disclosing personal information without reference to future uses to which that information might be put. After all, courts are not fortune-tellers. However, this does not bode well for youth privacy online. Youth privacy violations are almost certain to occur as new uses and technologies emerge and, thanks to their *ex post facto* reasoning, courts will be too late to prevent harm. Common sense and the precautionary principle support a conservative approach to youth privacy that evaluates the reasonableness of a particular collection, use, or disclosure of youths' personal information not just in the context of current circumstances, but with a view to possible future consequences. Anything less risks jeopardizing youth privacy by subjecting young people to surveillance for purposes that are only reasonable when one ignores the risk of future harm.

---

64 *Ibid*, Section 1 at paras 110–111.

65 *Turner v. Telus Communications Inc.*, 2007 FCA 21, [2007] 4 F.C.R. 368, 2007 CarswellNat 1175, 2007 CarswellNat 172 (F.C.A.).

66 *Ibid* at para 15.

Fifthly, the Office of the Privacy Commissioner lacks sufficient power to curtail youth privacy violations. The Commissioner makes recommendations and can apply to Federal Court to enforce those recommendations as an order of the court, but that process is both cumbersome and rarely used. The Nexopia investigation is a prime example of the Commissioner's deficiencies: Nexopia refused to follow 4 of 24 recommendations to comply with *PIPEDA*.[67] When the Privacy Commissioner sought to have the outstanding recommendations enforced in court, the owners sold the company. The new owners promised to make all changes by April 30, 2013; however, almost four years have passed since the complaint was filed and the OPC has yet to confirm whether all of its recommendations have been implemented.[68] Simply put, the Commissioner lacks the teeth it needs to enforce the *Act*. Related to the Commissioner's lack of enforcement power, the *Act* unduly burdens youth with the defence of their privacy. Although the Commissioner may audit the information management practices of websites on its own initiative, it is principally a complaint-driven body. As a result, *PIPEDA* places the onus on youth who feel that their privacy has been violated online — for example because a site failed to disclose a particular use of personal information or used it without consent — to take legal action against the company or else file a formal complaint with the Commissioner.[69]

Perhaps due to its lack of enforcement power, the OPC also appears to be too quick to defer to the practices of private organizations. Where an organization gives reasonable *notice*, it seems the Commissioner is willing to impute *consent* to the user. For example, in the Nexopia investigation, the Commissioner specifically noted the absence of pop-ups, click-through agreements, or help icons on the site as evidence that users may not have meaningfully consented to certain collections, uses, or disclosures of their personal information. When the site agreed to adopt these particular mechanisms, the Commissioner found this to satisfy its concern over obtaining consent.[70] The problem with these suggestions is that they are merely technical fixes to a nuanced problem. None ensure meaningful consent. Notices or pop-ups draw attention to an issue, but most youth do not read them because they are considered "long and boring."[71] Even if they do read them, they often do not understand.[72] In this way, the Commissioner's version of what will constitute consent resembles notice, rather than actual informed consent in the sense that an individual youth user appreciates the nature and consequences of sharing his private information online.

Lastly, it is not clear what will count as informed consent under the law because consent has not been defined. Must one understand not simply that his or her information is being used for marketing, but also every technical detail as to how

---

67 OPC, "Nexopia", *supra* note 7, Summary of Conclusions at para 6.

68 Office of the Privacy Commissioner of Canada, *Annual Report to Parliament 2012: Privacy and Your Reputation — Who Shapes Your Identity Online*? (Ottawa: OPC, 2013) at 18.

69 *PIPEDA*, *supra* note 10, s 11.

70 OPC, "Nexopia", *supra* note 7, Section 2 at paras 35 71, 74, 76.

71 Steeves, *supra* note 21 at 181.

72 Burkell, Micheti & Steeves, *supra* note 18 at 7.

the information is transmitted to accomplish that purpose? This is unlikely. However, using vague language that covers the kind of collection, use, or disclosure being employed has also been found to be inadequate.[73] The uncertainty of where along this spectrum meaningful consent will fall undermines respect for youths' informed privacy choices. In fact, it is uncertain whether or not youth can legally consent to the collection, use, and disclosure of their personal information *at all*. Principle 4.3 of *PIPEDA* requires knowledge and consent of the individual "except where inappropriate." The accompanying note in the *Act* suggests that it may be "impossible or inappropriate" to obtain consent when the individual is a minor.[74] At first glance, this would seem to create a loophole by which websites could collect youths' personal information without the need for consent. Complicating matters is the fact that youth under the age of 18 are also under a general incapacity to enter into contracts. A minor's parent or guardian is typically required to make decisions on the child's behalf.[75] This is consistent with the Privacy Commissioner's *Guide for Businesses*, which recommends that organizations obtain consent from a legal guardian.[76] However, it is *inconsistent* with the Privacy Commissioner's findings from the Nexopia investigation. In that report, the Commissioner said that websites should not focus on obtaining parental consent, but concentrate on obtaining the end user's consent instead:

> . . . there may be value in young users involving their parents in their online interactions, [but] the *Act* does not require the parents of all minors to consent to the collection, use and disclosure of personal information. Organizations who handle youths' personal information must explain their information handling practices in such a manner that youth can reasonably understand how their personal information will be used or disclosed. Accordingly, we have addressed issues relating to age and consent pursuant to this requirement.[77]

By sidestepping the issue of parents' role in supervising their children's online activities, the Privacy Commissioner implicitly acknowledges the practical difficulty of obtaining verifiable parental consent. Yet, at the same time, the Commissioner's emphasis on securing the consent of the individual youth directly contradicts testimony she gave in Parliament, where she openly doubted whether children could provide meaningful consent under *PIPEDA* at all.[78] It is ambiguous whether companies actually need consent to collect, use, or disclose a minor's personal information under *PIPEDA* and, if so, whether consent can or should be obtained from the parent or child. In the absence of greater clarity, websites will be able to skirt the rules and intrusions into youth privacy online will go unchecked. Therefore, the administration and interpretation of *PIPEDA* by the Privacy Commissioner and the courts raise serious concerns about the effectiveness of existing legislative protections for youth privacy online, and have elicited calls for reform.

---

73 *Ibid* at 61.

74 *PIPEDA*, *supra* note 10, Schedule 1, s 4.3.

75 Lawford, *supra* note 25 at 48.

76 OPC, *Guide for Businesses*, *supra* note 6 at 9.

77 OPC, "Nexopia", *supra* note 7, Section 2 at para 70.

78 House of Commons, *supra* note 16 at 98.

IV. PROBLEMS WITH PROPOSED REFORMS

The current law's ineffectiveness at protecting youth privacy online has led many to propose legislative reform. Unfortunately, these proposals are marred by their own problems, namely the fact that they operate within *PIPEDA*'s consent-oriented paradigm and fall victim to the same characteristic flaws of that system. The obsession with obtaining consent has reduced youth privacy online to a metaphorical (and, in some cases, literal) checkbox that websites need to get ticked, which misses the goal of privacy rights: to give users control over how their personal information is collected, used, and disclosed.

(a) Bill C-12

Section 29 of *PIPEDA* requires Parliament to review the *Act* every five years and propose changes as needed. The first round of review began in 2006, and on September 29, 2011 the federal government introduced Bill C-12 in the House of Commons, which would have been known as the *Safeguarding Canadians' Personal Information Act*.[79] The bill never made it to second reading and has not been reintroduced since the Prime Minister prorogued Parliament in September 2013. In response to concerns that *PIPEDA* did not sufficiently protect children's privacy, Bill C-12 would have amended *PIPEDA* to specify ". . . the consent of an individual is only valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting."[80] Industry Canada suggested this definition was chosen specifically because it would make obtaining the consent required to collect information from children more difficult.[81] In reality, however, this definition does not appear to add anything to *PIPEDA*'s existing requirement for meaningful consent. It simply makes explicit what the Privacy Commissioner already knows, which is that what constitutes meaningful consent for an adult may not be meaningful consent for a youth. The problem is that, even if Parliament adopted Bill C-12's definition, it does nothing to clarify whether parents can give consent on their child's behalf under *PIPEDA*, or whether the Privacy Commissioner's emphasis on obtaining the consent of the youth directly should be determinative. Furthermore, the definition cheapens youth privacy protections by infusing an objective analysis of whether it is "reasonable" to expect an individual to understand the nature, purpose, and consequences of the collection, rather than asking whether a particular youth or parent *subjectively* consented to the collection. Since privacy is inherently personal, its protection should not be dependent on an objective standard. Thus, Bill C-12 offers a technical fix to *PIPEDA*'s anaemic protections for youth privacy that (a) arguably does not help youth privacy and (b) fails to solve problems associated with the Office of the Privacy Commissioner.

---

79 Bill C-12, *An Act to amend the Personal Information Protection and Electronic Documents Act*, 1st Sess, 41st Parl, 2011 (first reading 29 September 2011).

80 *Ibid*, cl 5.

81 House of Commons, *supra* note 16 at 22.

(b) Bill C-475

The Standing Committee on Access to Information, Privacy and Ethics considered this latter problem in a 2012 study into the privacy practices of social media websites and heard testimony from companies including Facebook, Google, Nexopia, and Twitter. The committee issued a report in April 2013 titled *Privacy and Social Media in the Age of Big Data*.[82] As a result of that report, NDP committee member Charmaine Borg tabled a private member's bill, Bill C-475,[83] to enhance the Privacy Commissioner's enforcement powers. In particular, the bill would have given the Commissioner the power to make orders with the force of law and make it mandatory for all organizations to report data breaches.[84] This would greatly improve the Commissioner's ability to police and, if need be, punish website operators that violate youth privacy by forcing them to align with *PIPEDA*'s requirements. Still, two points are worth mentioning. First, opposition private members' bills are notoriously unsuccessful at winning Parliament's approval. Bill C-475 began second reading in May 2013 and, although it was reinstated after prorogation, the bill was ultimately defeated.[85] Second, these reforms do nothing to address the challenges with *PIPEDA* itself; they merely make it easier for the Privacy Commissioner to enforce a flawed statute. The issues of whether a minor can meaningfully consent and what counts as a reasonable use of youths' personal information remain unanswered. Hence, strengthening the Privacy Commissioner's powers, though desirable, does not address the underlying youth privacy challenge created by an equivocal legislative regime.

(c) Quebec's Consumer Protection Model

One way to bring clarity to the law on youth privacy online would be to adopt a model similar to the one Quebec has used for protecting children as consumers. That province's *Consumer Protection Act* has banned advertising to children under 13 with a few exceptions since the 1970s.[86] Irwin Toy challenged the constitutionality of the prohibition on the ground that it violated the company's freedom of expression under section 2(b) of the *Charter*. The Supreme Court of Canada agreed, but found that the limit was reasonable because other more minimally impairing means would not accomplish the objective of protecting children from exploitation by advertisers as effectively.[87] Although that case was decided in the context of consumer protection, a similar approach can be applied to youth privacy online. For instance, Valerie Steeves, a professor at the University of Ottawa, has

---

82 *Ibid.*

83 Bill C-475, *An Act to amend the Personal Information Protection and Electronic Documents Act (order-making power)*, 1st Sess, 41st Parl, 2013 (first reading 26 February 2013).

84 *Ibid*, cls 1(2), 2.

85 Bill C-475, *An Act to amend the Personal Information Protection and Electronic Documents Act (order-making power)*, 2nd Sess, 41st Parl, 2014 (defeated by the House of Commons 29 January 2014).

86 *Consumer Protection Act*, RSQ, c P-40.1, ss 248–249.

87 *Irwin Toy*, *supra* note 31 at para 88.

argued that banning websites from collecting, using, and disclosing personal information of youth below a certain age "may be the best way to protect kids from invasive online practices."[88] Steeves' position is driven by a concern about the adverse effects of surveillance in general. Under *PIPEDA*, no child is too young for a website to collect his or her information so long as the site obtains meaningful consent to the purposes for which the information is being collected. Since questions about the capacity to meaningfully consent most often arise with preteens, the Quebec model suggests that the only effective solution to safeguard youth privacy online is to prohibit websites from collecting their information at all. The problem with this blanket approach is that by instructing websites on what they cannot do, it inadvertently restricts what young people *can* do. In effect, this undermines youth privacy by denying youth a space to express themselves, often away from the prying eyes of parents. As one 17-year-old put it: ". . . I think privacy is more just you choosing what you want to keep to yourself. [. . .] And so I don't think that Facebook is violating privacy. I think it's letting people choose how they want to define privacy."[89] In other words, a prohibition model would deprive a whole group of youth of the choice to share their information online, not because they are each incapable of consenting to that choice, but because of assumptions attached to their age.

One might argue that the prohibition would only target commercial websites which have an economic interest in exploiting children's personal information for profit. Non-profit or government-operated websites could pop up to fill the void left by the ban and still allow youth to express themselves online.[90] This is true, but it misses the point: if youth online privacy is about choosing to share or not share personal information about oneself and thereby controlling what details are public and private, then it also assumes the right to choose with whom, on what platform, and on what terms (i.e. commercial or otherwise) a young person discloses that information. Therefore, shuttering online access for youth is as much a violation of their privacy as unauthorized uses of their personal information. In both cases, youth lose control based on generalized assumptions about their (in)ability to meaningfully consent to sharing their personal information online.

(d) The Children's Online Privacy Protection Act

In the United States, the *Children's Online Privacy Protection Act* (*COPPA*)[91] governs young people's privacy online. *COPPA* is distinct from *PIPEDA* in two important respects: first, the statute is specifically about children's privacy; and, second, it is specifically about privacy in an online context. Some advocates, including the federal NDP caucus, argue that Canada should adopt the Americans' approach of enacting online- and child-specific legislation to improve youth privacy protections.[92] However, one should not assume that child-specific legislation

88 Steeves, *supra* note 21 at 188.

89 Boyd & Marwick, *supra* note 14 at 11.

90 Richard, *supra* note 11 at 16.

91 *Children's Online Privacy Protection Act*, 15 USC §6501–6506 (1998) [*COPPA*].

92 House of Commons, *supra* note 16 at 98.

is inherently better than *PIPEDA*'s universal approach. The *COPPA* Rule requires website operators that target children or knowingly collect information from children under the age of 13 to first obtain "verifiable" parental consent prior to collecting the child's information online.[93] The US Federal Trade Commission, which administers the *Act*, has indicated that it will require a more reliable form of parental consent for websites that disclose children's information to third parties, thereby exposing children to greater risk of harm, than for those that advertise to youth without transferring their users' personal information.[94] Unlike the Quebec model, *COPPA* facilitates rather than prohibits the collection of personal information from youth under 13. This also means that, unlike *PIPEDA* where it is not clear if very young children or their parents could ever meaningfully consent to the collection of the child's personal information, *COPPA* puts the power squarely in parents' hands with one exception: *COPPA* does not require consent to collect the information of users aged 13 to 18. This renders teens vulnerable to unsolicited tracking and mining of their personal data.

The greatest problem with legislating custom privacy rules for youth is that it inevitably forces drafters into drawing bright lines based on age, which are virtually impossible to enforce. The American experience is instructive in this regard. In theory, Congress decided that youth under 13 were at a greater risk of harm to their online privacy and thus required the added safeguard of parental consent. In practice, many websites in the US have responded by not accepting users under 13 to avoid the added cost and difficulty of verifying consent.[95] For example, Facebook deletes approximately 20,000 accounts registered by users aged 12 and under every day.[96] This highlights how easy it is to lie about one's birthdate to circumvent the age restriction. It also means that, contrary to *COPPA*'s intention, websites are routinely collecting and selling personal information of youth younger than 13 without seeking parental consent.[97] Therefore, creating one set of online privacy rules for youth and a separate regime for adults has unintended consequences for youth privacy. Moreover, it jeopardizes youth privacy in the same way as the Quebec prohibition model in that it has the effect of shutting out the class of youth to whom a more stringent set of rules apply. As already discussed, denying youth access to commercial websites impinges on youths' ability to control who they share their information with, undermining youths' privacy online.

---

93 *COPPA*, *supra* note 91, §6502.

94 US, Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions* (July 2013) at H4, online: FTC <http://business.ftc.gov>.

95 Danah Boyd et al, "Why Parents Help Their Children Lie to Facebook About Age: Unintended Consequences of the '*Children's Online Privacy Protection Act*'", online: (2011) 16:11 First Monday 1 <http://www.firstmonday.org>.

96 Michael Oliveira, "Facebook has mulled opening social network to preteens", *The Globe and Mail* (20 October 2013) online: The Globe and Mail <http://www.theglobeandmail.com>.

97 Boyd et al, *supra* note 95.

(e) The Mature Minor

The Public Interest Advocacy Centre (PIAC) argues that privacy law ought to import the doctrine of the mature minor from the medical context. In *Manitoba (Director of Child & Family Services) v. C. (A.)*, the Supreme Court considered an appeal from a decision ordering a 14-year-old Jehovah's Witness to receive life-saving blood transfusions that she refused on religious grounds. The statutory presumption that it was in the "best interests" of minors 16 and older to defer to their wishes was upheld. However, the court also developed the concept of the "mature" minor: a child below the age of 16 who can appreciate the nature and consequences of a medical decision. According to the court's judgment, it is in a child's best interests that his or her views are increasingly determinative as maturity increases.[98] *AC* stands for the proposition that children have a right to a hearing before a judge to determine their relative maturity and whether they can appreciate the nature of the medical intervention.[99] PIAC suggests that a lower standard than the mature minor should be applied to youths' ability to consent to the collection of their personal information online because the latter is not a life or death situation.[100] Table 1 summarizes the group's proposal:

Table 1: Public Interest Advocacy Centre's Proposed Consent Requirements for the Collection, Use & Disclosure of Minors' Personal Information Online[101]

Age	**Consent**	**Disclosure to third parties allowed?**
12 and under	*Ban on collecting personal information*	
13 to 15	Teen + Parent	No
16 to age of majority	Teen	Yes, but need Teen + Parent to opt in

PIAC also suggests that websites should be compelled to purge all data collected from a youth upon reaching the age of majority unless the individual expressly allows the website to continue storing the information collected during his or her minority.[102] The result is a consent matrix consisting of varying demands on children and parents based on age. By instituting a graduated scheme of consent, the proposal recognizes a youth's greater maturity and independence as he or she increases in age. It also balances a youth's presumed level of maturity with checks on how their information can be used by websites, with disclosure to third parties demanding extra protection as the risk of information falling into the wrong hands increases.

98 *AC*, *supra* note 38 at para 116.

99 *Ibid* at paras. 114–115.

100 Lawford, *supra* note 25 at 72.

101 *Ibid* at 69–70.

102 *Ibid* at 72–73.

Despite PIAC's argument that a standard lower than the mature minor is desirable in the privacy context, the truth is that even if the mature minor was a more appropriate standard it would not be practical to administer. Society could not reasonably expect a youth to appear before a judge or some other administrative body to have his level of maturity assessed every time he wants to sign up for a new commercial website that has its own unique information management practices. Yet, in a perfect world, this would be the ideal solution to the challenge of respecting an individual's autonomy while ensuring the individual's privacy is protected by judging his ability to provide meaningful consent. It would be more minimally impairing to one's privacy and autonomy by tailoring prohibitions on web access and information disclosure to the unique developmental stage of each particular youth. However, privacy law should not try to approximate this tailoring based on arbitrary categories of age. In his dissent in *AC*, Binnie J. applied the constitutional test for arbitrariness, concluding:

> . . . the limit (i.e. the irrebuttable presumption [that youth below a certain age cannot consent to medical treatment]) when applied to young persons *of capacity* has "no real relation" to the legislative goal of protecting children who lack such capacity. The deprivation in the case of mature minors (a class to which A.C. belongs) is arbitrary, and the deprivation therefore violates s. 7.[103]

Binnie J. went on to find that the infringement of liberty and security of the person under section 7 of the *Charter* was disproportionate and not justified under section 1. The Justice's comments could be equally applied to PIAC's proposal that draws bright lines as to who can or cannot consent to the collection, use, or disclosure of their personal information. This prevents children who fall into one of these restricted age categories, but who are nevertheless capable of providing meaningful consent, from negotiating the boundaries of their privacy online. Abella J., writing for the majority, did not think the statute violated section 7 of the *Charter* because the "best interests" of children under 16 could also be construed as giving these youth the right to appear before a judge to prove they are sufficiently mature to make their own medical decisions. However, she agreed with Binnie J. that, in the absence of a hearing, it would be arbitrary to assume no one under 16 would ever have the capacity to grant or withhold consent to medical treatment.[104] In this way, by narrowly focusing on issues of age and consent, PIAC's proposal for reform makes arbitrary assumptions about the developmental capacity of youth. It will trap relatively mature youth in its rigid categories. Hence, as with defining consent under *PIPEDA*, strengthening the powers of the Privacy Commissioner, banning the collection of information from youth under 13, and *COPPA*'s separate privacy rules for children, PIAC's proposal usurps youths' own control over their private information, which is inconsistent with youths' positive conception of their right to privacy online.

---

103 *AC*, *supra* note 38 at para 223 [emphasis added].

104 *Ibid* at paras 107–108.

V. THE WAY FORWARD

The law has a role to play in protecting youth privacy online. The solution is not to lump all youth into categories based on assumptions about what they can or cannot consent to and then to deny them access to the tools they increasingly depend on for self-expression and discovery. Any answer depends on recognizing that the problem of youth privacy online is not a problem exclusive to youth. Two-thirds of adults who think website privacy policies are easy to understand also incorrectly believe that those sites will not share their information.[105] As already discussed, attempts to legislate child-specific privacy rules only serve to alienate youth from the online discussion. In the name of "protecting" youth from the evils of sharing personal information online, society might strip youth of the social media tools through which youth mediate their privacy. Simply put, youth privacy does not need protection if there is no privacy to be had. For reasons already mentioned, borrowing the doctrine of the mature minor from health law would be an ideal model to balance society's legitimate interest in protecting vulnerable children, while allowing mature youth to make their own choices about what information to share online. However, individualized assessment by a third party is not practical. Meanwhile, *COPPA* gives parents a say over whether their children under 13 can consent to collections of personal information, but seems to shut parents out of the decision-making for children 13 and older.

For all of these reasons, youth will experience privacy on the Internet most meaningfully when the decision to share personal information with commercial websites is made by youth themselves in conjunction with their parents. The law must give youth and parents the tools they need in order to manage a child's privacy online. These tools must be built into the systems architecture of all websites that collect, use, or disclose personal information, regardless of whether that information belongs to youth or adults. What is needed is nothing less than a privacy revolution: a change in how society does business and in how it conceives of the personal information people share. Only when society sees personal information as a birthright, rather than a commodity, will privacy be meaningfully respected. A multi-layered approach with a strong emphasis on education, supported by law, will be necessary to realize this goal.

(a) Privacy by Design

Instead of fretting over whether or not a certain collection, use, or disclosure of personal information is "reasonable" in the context of children, legislation should mandate that all commercial websites embed privacy protections into their systems. The former Information and Privacy Commissioner of Ontario, Ann Cavoukian, calls this "Privacy by Design" because it encourages developers to design their websites in a manner that has privacy in mind from conception to delivery.[106] Since privacy will be embedded into the web's architecture, adults and youth will benefit equally from its protections and youth will not be denied access to avoid compliance with a separate regulatory regime.

---

105 Steeves, *supra* note 21 at 182.

106 Ann Cavoukian, *Privacy By Design: Take the Challenge* (Toronto: Information and Privacy Commissioner of Ontario, 2009) at iv.

Such a mandate will likely attract opposition. For instance, as of October 2013, Facebook's default sharing settings for users between the ages of 13 and 18 is "Friends Only," as opposed to the broader "Friends of Friends" or "Public" settings.[107] Similarly, in September 2013 the Digital Advertising Alliance of Canada (DAAC) launched the Canadian Self-Regulatory Program for Online Behavioural Advertising. The program allows consumers to opt out of behavioural tracking by participating advertisers.[108] One can imagine companies lining up to argue that legislated privacy requirements are unnecessary because these organizations already provide means to protect user privacy. However, the problem with these self-regulatory approaches is that there is no way to guarantee compliance, and in both examples the companies only implemented these changes recently. Even then, Facebook and DAAC arguably only did so because they saw an economic advantage to improving youth privacy as a means to boost the confidence of its youth customers and their parents. It is not difficult to imagine an alternate scenario in which companies did not afford the same protections to youth so as to preserve profitability.

Privacy by Design does not mean all websites would have to adopt a "closed" network where all information is private by default. Rather, the expectation would be that all websites provide comprehensive and detailed privacy mechanisms that allow people to easily opt in or opt out of one or more purposes for which a website collects, uses, or discloses personal information. This would avoid the risks of "implied" consent when consent, as a matter of fact, was not actually present in the youth or parent. Websites may already voluntarily allow this to varying degrees, but under this proposal the law could require websites to list *all* purposes in one place and the choice to opt out would be available for each of these purposes individually. Websites could still list some purposes as conditions of service, in which case users should be notified that their account would be deleted if they want to opt out of those discrete uses. Importantly, these conditions would be transparent and could be revisited, instead of relying on one box ticked at registration. User control would become the default expectation among all users no matter what their age, using privacy as a lens through which the structural design of a website is assessed.

One might criticize this approach, as I have earlier in this article, on the basis that it is a technical solution to a deeper societal problem. As Cavoukian argues, however, technology is inherently neutral.[109] Even as it threatens privacy, new technologies can also be used to enhance privacy. In her 2011 Annual Report to Parliament on *PIPEDA*, the federal Privacy Commissioner suggested "many of the problems with [Nexopia] could have been avoided if only privacy considerations had been taken into account *back when the operation was being designed and*

---

107 Alexei Oreskovic, "Facebook lifts restriction on teen users sharing with public", *The Globe and Mail* (16 October 2013) online: The Globe and Mail <http://www.theglobeandmail.com>.

108 Digital Advertising Alliance of Canada, *Self-Regulatory Program For Online Behavioural Advertising*, online: DAAC <http://www.youradchoices.ca>.

109 Cavoukian, *supra* note 106 at iv.

launched."[110] If websites routinely implement privacy controls by design (and, under this proposal, by law), youth and their parents will be better equipped to avoid privacy intrusions.

(b) Parents as Judges

The thought of parents as judges of their child's best interests is enough to strike fear into the hearts of many teenagers. But it is unlikely parents will force a mass exodus of youth from the Internet. In fact, an American study has shown that parents are often complicit in allowing their children to register for websites like Facebook below the 13-year-old cut-off. Sixty-eight percent of parents admitted that they helped their underage child create a Facebook account and three out of every four of these parents knew that their child was registering against the site's rules. Moreover, 93% of all parents believe they should have the final say when it comes to regulating their child's web use.[111] These numbers might be lower in the Canadian context, adjusting for a more deferential political culture; but there is no reason to suspect that a substantial majority of Canadian parents would not also prefer to have a greater influence on their children's online activities. Witnesses at the Privacy Committee's study of social networks emphasized the need for parents to play a greater role in protecting their children online.[112] Clearly, there is a disconnect between the Privacy Commissioner's interpretation of *PIPEDA*, which could have the effect of restricting access for youth based on a perceived incapacity to meaningfully consent, and the role of parents in deciding what is appropriate for *their child*.

In the absence of judges assessing the relative maturity of youth and their capacity to consent to the collection, use, and disclosure of their personal information, parents are a natural alternative to make that determination. To the extent possible, this proposal avoids intruding on the privacy rights of mature youth who might otherwise lose control over what information they can share online due to attributed, rather than actual, assumptions about their capacity. Youth are not naïve. When they share personal information online, they do so as part of a calculated analysis based on risk and reward.[113] Furthermore, youth adopt social strategies to manage their privacy online, such as speaking in code to reach their intended audience, while leaving parents or advertisers in the dark.[114] It is always possible that parents will not let their child share information online, even if he or she is mature, but this is already true under *PIPEDA*. The law should not *force* parents to let their sons or daughters use Facebook, but it should be open to them to determine, in consultation with their children, whether it is appropriate for their children to share

---

110 Office of the Privacy Commissioner of Canada, *Annual Report to Parliament 2011: Privacy for Everyone* (Ottawa: OPC, June 2012) at 2 [emphasis added].

111 Boyd et al, *supra* note 95.

112 House of Commons, *supra* note 16 at 23.

113 Matthew Johnson, "From Protection to Empowerment: Reframing the Conversation on Youth Privacy Education" (Paper delivered at the Insights on Privacy Speaker Series, 8 September 2011), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca>.

114 Boyd & Marwick, *supra* note 14 at 18.

personal information online and, using the tools that would be required under a Privacy by Design law, to choose what purposes are acceptable to them.

One might argue it is unfair to expect parents to give informed consent to the collection of their child's information when privacy policies and terms of service are too complex for the average person to understand, far less to expect "mature" children to make that decision themselves. So the theory goes: modern western democracies have laws made by a professional class of legislators because a division of labour in society is most efficient. Citizens should defer to the legislature to make decisions and pass laws that prevent harm to society because policy issues are too complex for the average layperson — who is too preoccupied by personal affairs to be able to learn about the myriad ways in which personal information is collected, used, and disclosed by private organizations — to make an informed choice. The problem with this argument, however, is that it sidesteps the fact that adults are already expected to make decisions about their own privacy. Are lawmakers to establish tribunals to assess whether every adult has the capacity to understand the intricate information practices of the private sector every time one wants to sign up for a new website? Such a suggestion is both absurd and impractical as it ignores the important role for individual autonomy in making important choices.

A further objection can be made that giving discretion to youth and their parents to decide when it is appropriate for a youth to share personal information will harm children. Admittedly, this approach does not protect youth or their parents from underestimating the potential consequences of revealing youths' information online. It does not stop people from making poor choices. However, this is not necessarily a bad thing. For example, Canadian youth who reported having had a bad experience on Facebook were found to be more likely to control their information through the site's privacy settings.[115] In other words, there is something to be gained from allowing youth to experiment with their privacy online, to make mistakes, and to learn from them. One can tell a child not to touch the stove, but some children will not listen until they burn themselves. Denying youth this opportunity does a disservice to them. It is more harmful to act as though the law can solve all of society's ills when it cannot because, when Parliament does legislate and unintended consequences occur, the public loses confidence in the legal system. The solution to this dilemma is not to legally block youth from accessing websites that collect their information. Governments should focus on educating youth about the risks of sharing personal information online and use the law to give them the tools necessary to make privacy choices that work for them.

VI. CONCLUSION

Youth privacy online exists in a context where society has an interest in surveillance and technology makes it easier than ever before to collect, use, and dis-

---

115 Emily Christofides, Amy Muise & Serge Desmarais, *Privacy and Disclosure on Facebook: Youth and Adults' Information Disclosure and Perceptions of Privacy Risks* (26 March 2010) at 8, online: University of Guelph <http://www.psychology.uoguelph.ca/faculty/desmarais/files/OPC_Final_Report-Facebook_Privacy.pdf>.

close personal data. The economic benefits of tapping into the youth market have led commercial websites to track youths' online activity and exploit that information for private gain. Governments have been complicit in fostering a legal environment in which the commoditization of youths' personal information can continue. In some cases, the law has attributed vulnerability to youth as a class based on age, while in others it has considered the developmental capacity of each individual minor. Canada's *Personal Information Protection and Electronic Documents Act* supports youth privacy online by taking a broad approach to defining what personal information it will cover. *PIPEDA* requires websites to be honest about their reasons for collecting personal information and the statute is flexible enough to hold youth and adults to different standards, recognizing youths' particular vulnerability. On the other hand, the *Act*'s competing purposes of facilitating economic growth and protecting individual privacy have led the Privacy Commissioner to give special protection to youth in some instances and the same protection as adults in others. The Privacy Commissioner lacks effective powers to enforce the law and has failed to clarify whether parents' or children's voices are determinative in deciding who can or should be the one to "meaningfully consent" to the collection, use, or disclosure of a minor's personal information.

Unfortunately, many of the proposed reforms are preoccupied with ages of consent, a focus that paints all youth with a single brush. Prohibiting the collection of personal information from youth under 13 or child-specific legislation like *COPPA* in the US have the practical effect of denying youth access to commercial websites upon which they depend to express their identities. Youth experience privacy intrusions not only in a negative sense (e.g. a website collecting personal information without consent), but also in a positive sense (e.g. being deprived of the choice or preferred means of communicating personal information). In both cases, they lose control. The model of the mature minor would be an ideal way to moderate youth privacy online, but it would be impractical to administer. PIAC's alternative, a graduated matrix of consent requirements based on what *it* believes is appropriate for youth of a particular age, is not minimally impairing of youths' privacy interests. It would prevent youth who are mature enough to manage their own privacy from participating in the online community. As a result, it falls onto the shoulders of parents to decide what is appropriate for their child. This approach tailors privacy to the individual youth, instead of lumping all children together based on generalized assumptions about capacity. With a robust educational strategy and a legislative framework that emphasizes Privacy by Design, youth and parents will make choices that respect their own privacy, which is inherently personal and should not be constrained based on membership in a particular class. The common plea among youth advocates is always to "think of the children." But in thinking about the *children*, legislators would be wise to not forget the *child*.