The Inadequacies of British Columbia and Federal Privacy Legislation to Respond to the Practical Realities of Social Media

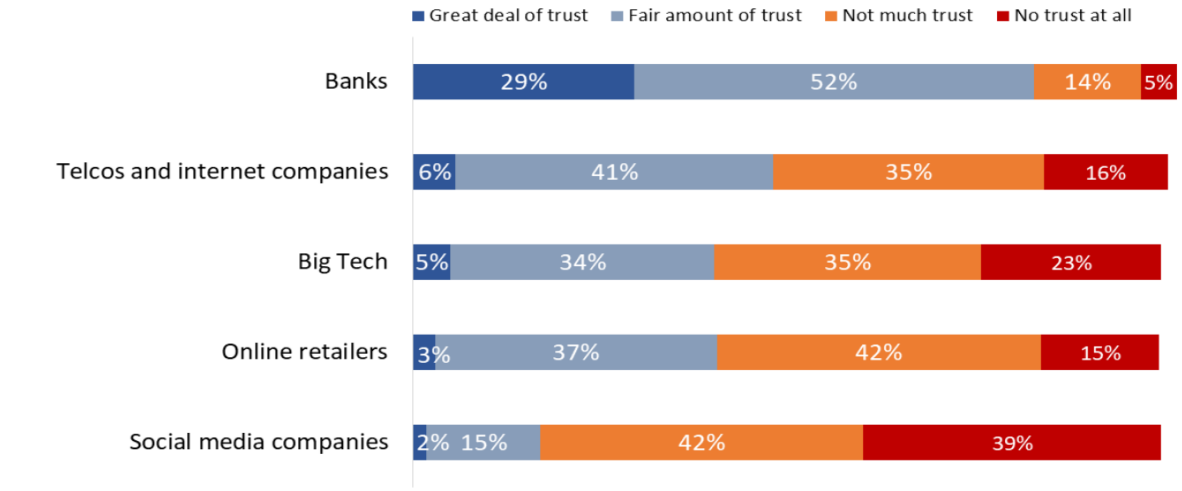
Olivia Startup

January 19, 2022

Introduction

Like it or not, social media has become an unavoidable aspect of everyday life. As of 2018, Statistics Canada reports, "social media use is prevalent across age groups, regularly used by about 9 in 10 Canadians aged 15 to 34 and by about 8 in 10 of those aged 35 to 49…6 in 10 of those aged 50 to 64 and about 1 in 3 seniors."[1] High rates of social media use persist despite associated risks to health, well-being, and privacy.[2] While the privacy implications of social media are not new, individuals continue to turn to social media time and again despite themselves expressing considerable concern over the privacy of the information they post online. "A three-year German study ending in 2012 showed that the more people disclosed about themselves on social media, the more privacy they said they desired."[3] Despite this, individuals "continued to participate because they were afraid of being left out or judged by others as unplugged and unengaged losers. So the cycle of disclosure followed by feelings of vulnerability and general dissatisfaction continued." A research survey conducted in 2020 on behalf of the Privacy Commissioner of Canada found 81% of Canadians do not trust social media companies much to protect their personal information or do not trust them at all. [4] As demonstrated in the figure below, compared to other private organizations, "Canadians were least likely to trust social media companies to protect their personal information" with only 2% trusting them a great deal and 15% with a fair amount of trust.[5]

Figure 7: Trust in different organizations to protect personal information



5. How much trust do you have in the following organizations to protect the personal information you share with them?
Base: n=1,502; Don't know: 2% or less

6

[1] Statistics Canada, *Canadians' assessments of social media in their lives*, by Christopher Schimmele, Jonathan Fonberg & Grant Schellenberg, in *Economic and Social Reports*, last modified 26 October 2021, (Ottawa: Statistics Canada, 24 March 2021), online: <www150.statcan.gc.ca/n1/pub/36-28-0001/2021003/article/00004-eng.htm>.
[2] *Ibid.*
[3] Monica Anderson and Jingjing Jiang, "Teens, Social Media and Technology 2018" (31 May 2018), online: *Pew Research Center* <https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/>.
[4] Office of the Privacy Commissioner of Canada, *2020-21 Survey of Canadians on Privacy-Related Issues*, Catalogue No IP54-109/2021E-PDF (Gatineau: OPC, 10 March 2021), online: <www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por_2020-21_ca/#fig01> [*Survey on Privacy-Related Issues*].
[5] *Ibid.*
[6] *Ibid.*

This can be compared to 45% of Canadians who generally trust private organizations to protect their privacy rights.[7] The vast majority of Canadians are also at least somewhat concerned about social media platforms gathering personal information that they (88%) or someone else (89%) posted online to create a detailed profile of their interests and personal traits."[8]

So what have Canadians done in response to these privacy concerns? Seventy-four percent (74%) "have adjusted privacy settings on a social media account."[9] It is unclear what impact this had on individuals' perception of their privacy on social media. "Far fewer have deleted a social media account due to privacy concerns (41%)."[10] However, this statistic does not account for which social media sites the individuals deleted or how many. Given that many individuals use a number of social media platforms (59.3% of Canadians reported using two or more),[11] it seems unlikely that these individuals have completely stopped engaging with social media altogether, but have rather switched platforms. The most concerning statistic of all: 61% of Canadians "feel they have not very much or no control at all over how their personal information is used by companies."[12]

In this paper, I will provide an overview of the ways in which personal information on social media is protected or not protected by private privacy legislation in British Columbia and Canada from both the social media organizations themselves and third-parties who seek to scrape personal information posted on social media. As I will demonstrate below, the legislation fails to adequately respond to the reality of common social media use. Social media's business model of trading in personal information, the practical limitations of individuals providing fulsome consent, as well as the necessity of organization compliance or extraterritorial enforcement have all outpaced the legislation. Although there are no readily apparent solutions to address some of these inconsistencies while simultaneously respecting individual autonomy and the businesses rights of the sites, I will suggest some reforms that will at least move privacy legislation in the right direction to ensure a greater degree of privacy protection on social media.

General Privacy Legislation Relating to the Collection, Use, and Disclosure of Personal Information

The way in which private organizations collect and use an individual's personal information is governed either by The *Personal Information Protection and Electronic Documents Act*[13] or by provincial privacy legislation which has been deemed substantially similar. The BC *Personal Information Protection Act*[14] has been deemed substantially similar,[15] and is therefore the applicable legislation in British Columbia. As will be demonstrated below, likely due to multijurisdictional nature of social media, the Privacy Commissioner of Canada has mostly addressed complaints under *PIPEDA*, often with the joint participation of other privacy

---

[7] *Ibid.*
[8] *Ibid.*
[9] *Ibid*.
[10] *Ibid.*
[11] *Ibid*.
[12] *Ibid*.
[13] SC 2000, c 5 [*PIPEDA*].
[14] SBC 2003, c 63 [*PIPA*].
[15] *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220.

commissioners such as the BC Privacy Commissioner.

Private organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.[16] Both Acts balance the right of individuals to protect their information and the needs of the organization.[17] The legislation is primarily consent-based; the organization must inform individuals of the purpose of collecting and using their information and obtain informed consent or implied consent.[18] Individuals also have the right to withdraw their consent.[19] Finally, "[a]n organization must not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service."[20]

Organizations are additionally required to keep information secure,[21] retain it only as long as it is necessary for its purpose,[22] as well as make a "reasonable effort to ensure" that all information they have about an individual "is accurate and complete."[23]

For enforcement, both commissioners have the power to investigate complaints under the legislation.[24] Under *PIPEDA*, the Commissioner can make recommendations, and under *PIPA* an order to comply with the legislation. If a party fails to comply with a recommendation or order, a party or the Commissioner can apply to a court for enforcement, in which the court can award damages under *PIPEDA,* or a fine of up to $10,000 for individuals and $100,000 for organizations under *PIPA*. [25]

Privacy Law's Application to Social Media

Application to Service Providers

The application of privacy law to social media sites is best exemplified in a series of decisions in relation to Facebook. In 2009, following a complaint from a public interest group, the Privacy Commissioner of Canada investigated Facebook's compliance with PIPEDA.[26] The Commissioner found Facebook was not complying on a number of fronts, including:

1. Default privacy settings that were not transparent on what information was being collected under the different privacy settings.
2. A lack of adequate information on advertising and which advertising options were required versus optional to use the service.

---

[16] *PIPA* ss. 11, 14, and 17, *PIPEDA* s. 5(3)
[17] *PIPEDA* s 3.
[18] *PIPA* ss 6-8.
[19] *Ibid* s 9.
[20] *Ibid* s. 7(2).
[21] *Ibid* s. 34.
[22] *Ibid* s. 35.
[23] *Ibid* s. 33.
[24] *PIPEDA* s. 12, *PIPA* s. 36(2).
[25] *PIPEDA* s. 16, *PIPA* s. 56(2).
[26] Office of the Privacy Commissioner of Canada, *PIPEDA Report of Findings #2009-008*, (OPC, 16 July 2009), online: <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-008/> [*Report #2009-008*].

3. A lack of safeguards to prohibit developers from accessing users' personal information and a lack of information on what third parties were able to access.
4. Failing to adequately explain the differences in retention of information for deactivation of an account and deletion of an account, the latter of which erases personal information from Facebook servers to the extent that is possible.[27]

In a follow up to the investigation a year later, the Commissioner concluded that Facebook had adequately amended its terms of use statement and privacy policy to provide individuals with adequate information on how their information was being used.[28] However, on one matter in particular the Commissioner noted, "The question of default settings for public search listing was more complex to assess because of significant changes to the site since the complaint was filed in May 2008," and "[u]ltimately, the Commissioner determined this issue to be outside the scope of the follow-up process for this investigation."[29] The Commissioner noted they continued to investigate a number of privacy complaints that were not raised in the report, so this issue may have been under separate investigation at the time but it was unclear.[30]

In 2018, the Commissioner received a complaint in relation to "Facebook's disclosure of the personal information of certain of its users to a third-party application…that was later used by third-parties for targeted political messaging."[31] The Privacy Commissioner conducted a joint investigation with the OIPC BC and held Facebook had violated PIPEDA in the following ways:

1. Facebook failed to obtain valid and meaningful consent of installing users.
2. Facebook also failed to obtain meaningful consent from friends of installing users.
3. Facebook had inadequate safeguards to protect user information.
4. Facebook failed to be accountable for the user information under its control.[32]

The Commissioner noted this contravention was particularly concerning in light of the Commissioner's previous finding in 2009 for very similar issues of "overbroad and uninformed consent for disclosures…to third party-apps, and inadequate monitoring to protect against unauthorized access by those apps."[33]

In relation to consent, the Commissioner held that "Facebook relied on overbroad and conflicting language in its privacy communications that was clearly insufficient to support meaningful consent."[34] The Commissioner held it was insufficient for Facebook to rely on consent for policies exclusively outlined on registration "in relation to disclosures that could occur years later, to unknown apps for unknown purposes."[35] Facebook was also unable to rely

---

[27] *Ibid*.
[28] Office of the Privacy Commissioner of Canada, *Facebook investigation follow-up complete*, (Ottawa: OPC, 22 September 2010), online: <www.priv.gc.ca/en/opc-news/news-and-announcements/2010/bg_100922/> [*Facebook investigation follow-up*].
[29] *Ibid.*
[30] *Ibid*.
[31] PIPEDA Report of Findings No 2019-002, [2019] CPCSF No 2, [2019] SCCPVPC no 2 (OPC) at para 1 [*Report of Findings No 2019-002*].
[32] *Ibid* at para 4.
[33] *Ibid* at para 5.
[34] *Ibid* at para 4.
[35] *Ibid* at para 4.

on the third party apps to obtain consent for disclosure because it was unable to demonstrate the app had "actually obtained meaningful consent for its purposes, including potentially, political purposes" and Facebook had failed to make reasonable efforts to ensure the apps "were obtaining meaningful consent from users."[36] It was additionally unreasonable for Facebook to use installing users' consent to obtain information from that user's friends "even though the friends would have had no knowledge of that disclosure."[37]

In relation to adequate safeguards to protect information, the Commissioners held,

> Facebook relied on contractual terms with apps to protect against unauthorized access to users' information, but then put in place superficial, largely reactive, and thus ineffective, monitoring to ensure compliance with those terms. Furthermore, Facebook was unable to provide evidence of enforcement actions taken in relation to privacy related contraventions of those contractual requirements.[38]

In essence, Facebook was attempting to avoid its responsibilities of obtaining meaningful consent and protecting users' personal information by "shifting that responsibility almost exclusively to users and Apps."[39] Rather, its "overbroad consent language" and lack of implementation of consent mechanisms and safeguards "resulted in a privacy protection framework that was empty."[40]

Facebook has since refused to implement the Commissioner's recommendations and the Commissioner subsequently brought an application to the Federal court seeking an order requiring Facebook to comply with the legislation, which is still before the courts.[41]

Application to Third Parties and Scraping

In addition to an individual's privacy rights in the context of the contractual relationship with the service provider itself, *PIPA* and *PIPEDA* extend to personal information that is posted online and collected, used, or disclosed by third parties without the user's knowledge, a process called scraping.[42] For example, in a report on the ways in which Canadian political parties use personal information, the Commissioner clarified,

> When an individual directly communicates with a political party using social

---

[36] *Ibid* at para 4.
[37] *Ibid* at para 4.
[38] *Ibid* at para 4.
[39] *Ibid* at para 4.
[40] *Ibid* at para 4.
[41] Office of the Privacy Commissioner of Canada, *Notice of Application with the Federal Court against Facebook, Inc.*, 6 February, 2020, (Gatineau: OPC), online: < https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-complaints-and-enforcement-process/court_p/na_fb_20200206/>; Office of the Privacy Commissioner of Canada, *Certificate of nomination of Daniel Therrien to the position of Privacy Commissioner Issue Sheets*, (OPC), online: <www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/ethi_20210621/is_ethi_20210621/#toc18>.
[42] Bogdan Batrinca & Philip C. Treleaven, "Social media analytics: a survey of techniques, tools and platforms" (26 July 2014, *AI & Soc* 30, 89-116 (2015).

> media, a party may collect and add that information to their database for the purpose of communicating with that individual. The collection for this purpose is authorized by implied consent, because the user understands the nature of the platform and has voluntarily communicated with the party.
>
> However, use of this information beyond the purpose of communication, such as voter profiling or scoring, is likely not authorized by PIPA without express consent.[43]

Furthermore, an individual liking "or shar[ing] information about a political party on social media" does not constitute "consent for the party to collect the individual's personal information," noting, "[i]f the individual does desire further interaction with the party, it is very easy for them to do so."[44] The Commissioner concluded that a number of the political parties had failed to obtain proper consent and recommended they ensure they do so.[45]

One of the most concerning applications of scraping is where online personal information may be used in the context of employment, specifically in deciding whether or not to hire an individual. This use of personal information by employers could have serious, tangible, and long-lasting effects on one's ability to be employed in their selected field. There is no explicit jurisprudence regarding an employer's search of a prospective employees social media presence, but the Privacy Commissioner has made it clear that organizations or public bodies that do so are subject to *PIPA* (or the *Freedom of Information and Protection of Privacy Act*[46] for public employers in BC), regardless of whether the information is publicly or privately available.[47] This would mean that the employer's reason for collecting and using the social media information would have to be considered appropriate in the circumstances. As the Commissioner additionally notes, there is a duty on organizations to ensure the information they collect is accurate, "whether the employer is viewing information or if they save copies of the information."[48]

While the employer can attempt to gain the consent of the individual to access their social media accounts, the Commissioner also highlighted that an over-reliance on consent may not be sufficient to comply with the Act.[49] Under *PIPA*, even if the employee provides consent, the collection will still have to be reasonable.[50] As an example, the Commissioner notes that it would be unreasonable for an employer to collect information from an online dating profile "in most circumstances."[51] In addition, individuals are able to withdraw their consent, in which case "the organization must not use that information to make a decision about that individual."[52] The Commissioner additionally notes an employer would be entitled to collect and use information even without an individual's consent where the information "is about that individual's

---

[43] Investigation Report No P-19-01, 2019 BCIPC 7 at 21.
[44] *Ibid* at 21.
[45] *Ibid* at 21.
[46] [RSBC 1996] c 165 [*FIPPA*].
[47] Office of the Information & Privacy Commissioner for British Columbia, *Conducting Social Media Background Checks,* May 2017 update (Victoria: OIPC) at 1 and 4 [*Conducting Background Checks*].
[48] *Ibid* at 2.
[49] *Ibid* at 3.
[50] Additionally, public employers regulated by *FIPPA*, consent does not override the requirement for the information to the necessary for an operating program or activity of the public body (*ibid* at 3).
[51] *Ibid* at 3.
[52] *Ibid* at 3.

employment" and it could be used "for reasonable purposes relating to recruiting, establishing, managing, or terminating the employment or volunteer relationship."[53] The only example the commissioner offers is "if an employer sees a Facebook posting by an employee that contains proprietary company information."[54] Even if the employer may come across relevant information that they are entitled to collect or that they have been provided consent to collect, they may inadvertently collect too broad an array of personal information or the personal information of third parties.[55]

Privacy legislation has also been applied in circumstances where a third party has directly interacted with a user's social media profile, rather than scraping the information after the fact. In several cases against the organization Surrey Creep Catcher, the BC Privacy Commissioner held the organization had breached *PIPA* for collecting and posting information about the claimants online. [56] The organization acted as a vigilante group and posted online messages and video footage of meeting in person as alleged proof of the individuals committing the crime of luring minors for sexual purposes. The Commissioner in each case held the organization did not obtain proper consent for the collection and disclosure, they did not provide them with the true intended purpose of the collection and disclosure when they explained their purposes for recording the interaction, and any consent would have been nullified by the "deceptive" practices of the organization.[57] As a result, the Commissioner ordered the organization to destroy all copies of the records and remove all relevant content from the internet.[58] In Order P17-03, the Commissioner additionally ordered the organization to "[r]equest, and ensure to the extent possible, that anyone encouraged to post or share [the Complainant's] personal information removes it from the internet and destroys it" as well as "[r]equest that the Service provider operating the host site of any of the foregoing personal information of [the Complainants], whether Facebook, YouTube, or any other service provider, remove the information from its site."[59] Interestingly, in the later case, Order P20-05, the adjudicator made no such order.

The Inadequacy of Privacy Legislation to Respond to Privacy Concerns on Social Media

Legislation Not Responsive to the Business Format and Practical Realities of Social Media Use

While the various reports and findings of violations against social media sites are not insignificant, they nonetheless demonstrate the limitations of privacy legislation to adequately respond to the practical realities of social media. The very premise of social media is to deal in people's personal information.[60] As a result, the traditional consent-based model of private privacy legislation cannot function properly. The requirement that consent cannot be required to provide a service is rendered useless in this context since an individual's personal information is necessary for the social media business model. This consent-based model also fails to take into

---

[53] *Ibid* at 3.
[54] *Ibid* at 3.
[55] *Ibid* at 3.
[56] Order P17-03, 2017 BCIPC 38 and Order P20-05, 2020 BCIPC 33.
[57] Order P17-03 at paras 41-47.
[58] *Ibid* at para 65.
[59] *Ibid* at paras 65, 67.
[60] Matthew Rosenberg & Gabriel J.X. Dance, "'You Are the Product': Targeted by Cambridge Analytica on Facebook" (8 April 2018), online: *The New York Times* <www.nytimes.com/2018/04/08/us/facebook-users-data-harvested-cambridge-analytica.html> .

account the practical realities of social media use. Our social and even business interactions have become increasingly built around these sites. Consumers additionally have very minimal contractual power which is limited to either accepting or rejecting the standard form contracts provided by these companies. Freedom of choice is even further reduced when an individual feels they will be excluded from society in some way if they do not participate in such activities. Even if companies were to implement more meaningful consent policies, this would likely just lead to an increase in consent fatigue and reduce the chances that individuals will engage with the privacy policies at all. One study indicates that, contrary to popular belief, "privacy fatigue has a stronger impact on privacy behaviour than privacy concerns do."[61] It is also practically impossible to expect all individuals to read the privacy policies of every online platform. A study conducted in 2008 found "that reading the privacy policies of just the most popular websites would take an individual 244 hours – or more than 30 full working days – each year."[62]

Another driving factor in why the consent-based privacy model cannot properly work in the social media context is the overall lack of privacy law and internet literacy. Since most people do not read privacy policies before agreeing to the contractual terms, most do not understand what they are agreeing to and in turn may not appreciate what social media companies can legally demand. Nearly two-thirds of Canadians…rated their knowledge of their privacy rights as good (50%) or very good (14%)."[63] However, this was self-reported and the study did not engage with whether the individuals questioned did in fact know their privacy rights. Considering that 61% felt they do not have much control or no control over how their personal information is used by companies, it seems unlikely that these individuals are as well informed as they believe.[64] Smaller organizations themselves are also likely unaware of the privacy implications every time they conduct a google search and retain personal information.

Furthermore, even if individuals were able to have more control over their privacy boundaries on social media, this would not resolve issues of internet literacy. Given the break-neck speed with which technology and the internet has evolved, it is no surprise that a large number of individuals, particularly those raised without social media, would struggle to fully comprehend how it functions and how to best protect their information. For example, while 88% of Canadians under 35 reported adjusting their privacy settings, only 51% of those 55 and up reported doing so.[65]

Issues of Compliance and Extraterritorial Enforcement

Even in the context of scraping, which affords protection regardless of consent, issues of detection, compliance, and enforcement on a platform like the internet can limit or even negate a claimant's relief. As noted above, in Order P17-03, the BC Commissioner ordered the

---

[61] Hanbyul Choi, Johnghwa Park & Yoonhyuk Jung, "The role of privacy fatigue in online privacy behaviour" *Computers in Human Behaviour*, vol 81, April 2018, p 42-51.

[62] Fred H. Cate, Peter Cullen & Viktor Mayer Schonberger, "Data Protection Principles for the 21st Century" (2013). *Books by Maurer Faculty*. 23 Mauer School of Law: Indiana University. <www.repository.law.indiana.edu/facbooks/23?utm_source=www.repository.law.indiana.edu%2Ffacbooks%2F23&utm_medium=PDF&utm_campaign=PDFCoverPages> , referencing Aleecia M. McDonald & Lorrie Faith Cranor, "The Cost of Reading Privacy Policies" (2008) 4:3 ISJLP 543.

[63] *Survey on Privacy-Related Issues, supra* note 4.

[64] *Ibid.*

[65] *Ibid.*

organization to request anyone who shared the content to remove it, as well as request the service providers themselves to remove it. While this sounds like a desirable outcome, it is implausible to chase down every individual who copied the content or commented on it, and the organization making a general post to request their friends or followers to do so is unlikely to be effective. Similarly, the likelihood of social media companies being able to successfully remove the content is equally slim. Even if they were willing to remove the content, the artificial intelligence currently used to do so is highly flawed. Internal Facebook documents demonstrate "AI has only minimal success in removing hate speech, violent images and other problem content" estimating that only 2% of hate speech on the platform that violated its rules was removed.[66] So while Facebook may be able to target information when provided explicit instructions on who has posted it, its ability to identify the content when reproduced elsewhere on the site is likely to be highly unsuccessful. This is also likely exacerbated by the fact that removed content can simply be reposted. This not only minimizes the chances of compliance but could also potentially discourage individuals from enforcing their privacy rights if they are repeatedly forced to bring the matter back to the Commissioner.

Another major barrier to compliance is the issue of international private law. All prevalent social media sites are not situated in Canada, and while the principle of comity encourages courts to defer to orders where jurisdiction has been properly taken,[67] this is not a legal requirement,[68] thus making the enforcement of Canadian rulings incumbent on foreign courts' willingness to do so.

While *Google Inc. v Equustek Solutions Inc*,[69] dealt with intellectual property rights rather than privacy, it nonetheless demonstrates the challenges and barriers of enforcing orders on global platforms. In this case, Equustek sued its former distributor for misappropriating its intellectual property by selling Equustek's products as its own. The distributor abandoned proceedings and left the country, refusing to comply with court injunctions to stop selling the prohibited products until the resolution of the proceedings. Equustek sought to have google de-index the distributor's websites. Google only de-indexed websites on its Canadian platform, and had not de-indexed all of their websites, enabling the distributor to circumvent the order by moving its products to its other websites. As a result, the Supreme Court of Canada ordered Google to globally de-index the distributor's websites. Google challenged the extraterritorial effect of the order, but the court held Google's compliance with the order was necessary in order to ensure general compliance with the injunction and prevent irreparable harm in light of Google's important function in accessing online information.[70] In support of this, Abella J. noted, "The Internet has no borders — its natural habitat is global. The only way to ensure that the interlocutory injunction attained its objective was to have it apply where Google operates — globally."[71] This reasoning is a perfect example of the law being adapted to accommodate the realities of modern technology and internet use and could be similarly applied in privacy related

---

[66] Deepa Seetharaman, Jeff Horwitz & Justin Scheck, "Facebook Says AI Will Clean Up the Platform. Its Own Engineers Have Doubts." (17 October 2021), online: *The Wall Street Journal.* <https://www.wsj.com/articles/facebook-ai-enforce-rules-engineers-doubtful-artificial-intelligence-11634338184>.
[67] *Morgaurd Investments Ltd v De* Savoye, [1990] 3 SCR 1077 at 1095, [1990] SCJ No 135.
[68] Antika Gupta, "*Google v Equustek*: An Attempt to Domestically Govern a Global Resource" (16 October 2017), online: *The Court* <www.thecourt.ca/google-v-equustek-an-attempt-to-domestically-govern-a-global-resource/>.
[69] 2017 SCC 34 [*Equustek*].
[70] *Ibid* at paras 34 and 18.
[71] *Ibid* at para 41.

incidents. The problem however, is that such reasoning is rendered moot unless the relevant foreign court is willing to enforce the order. In response to the SCC's finding, Google sought an injunction from the order from a United States' Federal Court.[72] The U.S. court refused to uphold the SCC decision on the basis that it was contrary to a law entitling Google to immunity from liability for the publishing content of a third party, depriving Google "of the benefits of U.S. Federal law." It also held it would undermine the public interest of the legislation to ensure "free speech on the global internet."[73] While the SCC decision remains good law, it is has nonetheless been rendered ineffective.

Lack of foreign enforcement can additionally have far reaching impacts on companies' willingness to cooperate with Canadian courts or privacy commissioners, as exemplified by the distributor in *Equustek*. Report No 2019-002 offers another example of this, in which the Commissioner noted Facebook was uncooperative during the investigation process by not answering many of their questions or providing incomplete or deficient answers.[74]

Ultimately, extraterritorial enforcement is an issue that the privacy commissioners in Canada have been contending with for years. The BC Privacy Commissioner acknowledged this tension in 2012 submissions to the House of Commons Standing Committee on a study into privacy and social media, while understandably offering no means to address it.[75] In light of the legal principle against laws applying extraterritorially,[76] the only feasible solution to foreign enforceability is through international regulation of the internet or intergovernmental agreements with jurisdictions where social media companies are located, which is predominantly California. The feasibility and challenges of such an endeavour are beyond the scope of this paper.

Social media blurring the boundaries between public and private spaces

In *R v Jarvis*,[77] the Court held, "'privacy', as ordinarily understood, is not an all-or-nothing concept, and being in a public or semi-public space does not automatically negate all expectations of privacy with respect to observation or recording." So too is the case on social media: third parties are not entitled to information posted online just because it is public. The very format of social media however, is designed to blur the boundaries between public and private, likely blurring the distinction between the legal right to privacy and societal expectations of privacy. Individuals are encouraged to share personal and intimate content about themselves: from photos to lifestyle blogs, and large life status updates to small inconsequential happenings of people's daily life. As noted by the Office of the Privacy Commissioner of Canada (OPC), "What we think, what we read, what we search, where we are, what we buy—once our own

---

[72] *Google LLC v Equustek Sols Inc*, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017).
[73] *Ibid*.
[74] *Report of Findings No 2019-002, supra* note 31 at para 3.
[75] See Office of the Information & Privacy Commissioner, *Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics Study: Privacy and Social Media*, (OIPC, 7 June 2012), online (pdf): *Office of the Information & Privacy Commissioner of BC* <https://www.oipc.bc.ca/legislative-submissions/1277> at 2-3.
[76] Gupta, *supra* note 68.
[77] 2019 SCC 20 at para 41.

business, is now everyone's business."[78] Several platforms continue to implement default privacy settings which automatically set accounts to public and require the user to opt-in to a private account.[79] This enables companies to benefit off individuals who are either too lazy to change their privacy settings or lack the internet literacy to do so.

More recently, the monetization of social media – whether through sponsorship opportunities and referral links for accounts with large followings,[80] content creator funds, or monetization of the sites themselves like YouTube[81] and TikTok[82] with many other sites following suit[83] – has effectively incentivised individuals to opt for the most public account possible. The larger the audience and the more captivating information an individual can share, the greater the chances of going viral. As Anita L. Allen, professor of law and philosophy at the University of Pennsylvania Law School, noted in an interview with New York Times journalist, Kate Murphy, "There's also this idea in our society that if I just embarrass myself enough I can be the next Snooki or Kardashian…There's a real financial incentive to not care and give it all up."[84] In her article, Murphy asserts what likely many individuals believe, despite what privacy legislation and the commissioner otherwise argue; that "There is no privacy" on the Internet.[85] Murphy further asserts, "it's hard to argue for the value of privacy when people eagerly share so much achingly personal information on social media."[86] This type of attitude, which is not uncommon, is dangerous because it perpetuates the idea that one should not expect any privacy online. This in turn encourages third parties to feel entitled to use personal information contrary to privacy legislation while simultaneously discouraging social media users from believing they have a legitimate privacy interest that could be enforced. This is reflected in the common adage: "be careful what you post online because the internet is forever.[87] The OPC acknowledged as much in outlining its strategic privacy priorities for 2015-2020, including reputation and privacy in light of the difficulty of removing content once posted online.[88] When you are constantly told you should expect your public social media to be used against you, why would you believe the law is going to protect you? Therefore, by trying to guard against the dangers of social media, we may be decreasing our confidence in privacy legislation and increasing ambivalence towards

---

[78] "The strategic privacy priorities*,"* last modified 14 December 2018, online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/about-the-opc/opc-strategic-privacy-priorities/the-strategic-privacy-priorities/#reputation>.
[79] "Continuing to Make Instagram Safer for the Youngest Members of Our Community" (17 March 2021), online: *Instagram*, <https://about.instagram.com/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community> ["Continuing to Make Instagram Safer"].
[80] Carsten Schwemmer & Sandra Ziewiecki, "Social Media Sellout: The Increasing Role of Product Promotion on YouTube" (14 August 2018) 4:3 Social Media + Society.
[81] "YouTube Partner Program overview & eligibility," online: *YouTube Help* <support.google.com/youtube/answer/72851?hl=en>.
[82] "Creator Fund," online: *TikTok* <https://www.tiktok.com/creators/creator-portal/en-us/getting-paid-to-create/creator-fund/>.
[83] See Facebook's for example: "Investing $1 Billion in Creators" (14 July 2021), online: *Meta* <about.fb.com/news/2021/07/investing-1-billion-dollars-in-creators/>.
[84] Kate Murphy, "We Want Privacy but Can't Stop Sharing" (Oct 4 2014), online: *The New York Times* <www.nytimes.com/2014/10/05/sunday-review/we-want-privacy-but-cant-stop-sharing.html>.
[85] *Ibid.*
[86] *Ibid*.
[87] Ramona Pringle, "Youth is no defence when it comes to shameful online posts" (16 June 2017), online: *CBC* <www.cbc.ca/news/opinion/youth-is-no-defence-when-it-comes-to-shameful-online-posts-1.4160070>.
[88] "The strategic privacy priorities," *supra* note 78.

those who seek to afford themselves of its protection after being seemingly "reckless" online.

The Impact on Minors and Future Implications

Minors are particularly vulnerable given their lack of legal literacy and ability to appreciate the long-reaching impact of posting content online. In a draft position on online reputation, the Privacy Commissioner of Canada argued teens and children "often have little or no option but to engage online" due to factors such as "social pressures or requirements placed on them by schools."[89]

Studies have linked higher rates of social media use in youth with increasing smartphone access. In 2020, 96.3% of 15 to 24 year-olds reported having a smartphone for personal use and 70.6% reported checking their smartphone at least every 30 minutes.[90] There is evidence to suggest the younger generation generally feels more confident about their privacy rights and less concerned about the privacy implications of social media. Generally, the younger one is, the more likely they are to report at least a fair amount of trust in social media companies to protect their personal information,[91] more likely to have adjusted their privacy settings,[92] more likely to report a great deal or moderate amount of control over how their personal information is used by companies,[93] and less likely to express concern about social media platforms gathering personal information that they or someone else posted online to create a detailed profile of their interests and personal traits.[94]

While on the one hand, these statistics could speak to better internet literacy when compared to older generations who did not grow up with modern technology, these studies fail to take into account the fact that children are on social media much younger than 15 or 16, which could have serious impacts on their ability to comprehend their privacy implications. Due to stricter legislation pertaining to children under 13 in California,[95] popular social media companies universally require users to be 13 years old.[96] However, in 2011 alone, Consumer Reports estimated that 7.5 million of the 20 million minors who used Facebook that year were underage in violation of these policies.[97] There is also additional evidence that children do not

---

[89] Office of the Privacy Commissioner of Canada, *Draft OPC Position on Online Reputation*, last modified 26 January 2018, (Gatineau: OPC), online: <www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/pos_or_201801/#heading-0-0-5> [*Draft OPC Position on Online Reputation*].

[90] Statistics Canada, *Table 22-10-0143-01 Smartphone personal use and selected habits by gender and age group*, (Ottawa: Statistics Canada, June 22, 2021), online: <https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=2210014301&pickMembers%5B0%5D=3.1&pickMembers%5B1%5D=4.2&cubeTimeFrame.startYear=2018&cubeTimeFrame.endYear=2020&referencePeriods=20180101%2C20200101>.

[91] *Survey on Privacy-Related Issues*, *supra* note 4, 24% of 16 to 24 year olds as opposed to 17% of Canadians of all ages above 16.

[92] *Ibid*, 88% as opposed to 51% of those over 55 years old.

[93] Ibid, "16 to 24 year olds (53%) compared to 35 to 54 year olds (36%) and those aged 55+ (33%)."

[94] *Ibid.*

[95] *Children's Online Privacy Protection Act*, 1998, 15 USC 16501-6505, 16 CFR Part 312 [*COPPA*].

[96] See Pavni Diwanji, "How Do We Know Someone Is Old Enough to Use Our Apps?" (27 July 2021), online: *Meta* <about.fb.com/news/2021/07/age-verification/>.

[97] "CR Survey: 7.5 Million Facebook Users are Under the Age of 13, Violating the Site's Terms" (May 10, 2011) Consumer Reports, online: <https://www.consumerreports.org/media-room/press-releases/2011/05/cr-survey-75-million-facebook-users-are-under-the-age-of-13-violating-the-sites-terms-/>.

fully appreciate the privacy implications of their social media use. For example, in one study, while children were able to appreciate the flow of information "in interpersonal contexts" where they provide the information, they have little appreciation for "the take-it-or-leave-it offer of commercial services, or the over-their-head management of their data by institutions" and "don't generally think of these as…[engaging] privacy."[98] Furthermore, they found,

> children are becoming aware of commercial uses of data traces. They know, for instance, that if they search for trainers, they will be served advertisements for trainers thereafter. But their awareness of inferred data and its value to business (or its long-term implications for them personally) is a different matter, and is dependent on their developing understanding of the business models operating in commercial and institutional contexts.[99]

Ultimately, despite self-proclamations of confidence in their ability to control their personal information on social media, these studies suggest that the omnipresence of social media use from such a young age has rather desensitized youth to its privacy implications.

Additionally, privacy legislation fails to address the complicated dynamic of parents posting personal information of their children before they are legally able to consent. Parents act for their children before they are of legal capacity,[100] whether that be the age of majority or when a mature minor seeks to assert their privacy rights.[101] This leaves children with entire online presences that they did not ask for and potentially do not want.

Potential implications of the widespread use of social media from such formative ages raises concerns not only for the individuals themselves, but also concerns for increased ambivalence towards online privacy and even potentially a shift in judicial interpretation of what constitutes "reasonable" collection, use, and disclosure. In this case, time will only tell.

Rapidly changing social media behaviours and technology

Section 3 of *PIPEDA* describes the privacy legislation's purpose in light of "an era in which technology increasingly facilitates the circulation and exchange of information." Although the legislation may not reflect this in practice, it is a crucial consideration given the rapid speed at which changing social media behaviours and advancing technology can create new or deepen privacy concerns online. In 2018, Pew reported,

> The social media landscape in which teens reside looks markedly different than it did as recently as three years ago. In the Center's 2014-2015 survey of teen social media

---

[98] Sonia Livingstone, Mariya Stoilova, & Rishita Nandagiri, "Talking to children about data and privacy online: research methodology" (6 September 2018) online: *London School of Economics and Political Science, Department of Media and Communications* <blogs.lse.ac.uk/parenting4digitalfuture/2018/09/06/theorising-privacy-how-do-and-how-should-children-know/> .

[99] *Ibid.*

[100] *Personal Information Protection Act Regulations*, BC Reg 473/2003 s 2(2).

[101] See for example Order P21-01, 2021 BCIPC 06 at para 18, in which the adjudicator held the claimant's daughter, who was thirteen at the time of the initial access request and 16 at the time of the decision, was a mature minor and capable of controlling her own privacy interests under the legislation.

> use, 71% of teens reported being Facebook users. No other platform was used by a clear majority of teens at the time.
>
> […]
>
> In 2018, three online platforms other than Facebook - YouTube, Instagram and Snapchat - are used by sizable majorities of this age group. Meanwhile, 51% of teens now say they use Facebook.[102]

These changes are not insignificant since the targeted content of each app can vary widely despite some general overlap. For example, with the shift to Instagram, "The app became a place where people mostly presented what they'd created or experienced, rather than posting about the day's outrage," making it a much more intimate setting, while Facebook continued to dominate as a platform for news and political opinion.[103] Snapchat's entire premise on the other hand, is that photos sent to friends vanish within seconds, which can encourage vulnerable minors to send very sensitive or embarrassing content to one another despite the real possibility of someone screenshotting the photo.[104] Simultaneously, technology is making it easier for third parties to obtain and use information in ways individuals would not have conceived of when they posted the content.[105]

The Challenge of Detecting Improper Use of Online Personal Information

The practical reality is, it is fast and easy to conduct a google or social media search and find any publicly available social media content, and once the information is discovered the damage is likely done. Even if third parties like employers were to act in accordance with legislation and obtain consent prior to collection, there are still inherent challenges if the individual were to withdraw consent. Once the information has been obtained, such knowledge cannot be unlearned, and it is hard to believe an employer would disregard information they otherwise would have used in making a hiring decision.[106]

Additionally, even if privacy legislation is applicable, in this context compliance is difficult to track and violations are extremely difficult to identify. Unless an employer were to openly admit they conducted a social media background check and used that information in making a decision in relation to a prospective employee, most would be completely unaware that the employer had ever even searched their information. This could have a distinct discriminatory impact on those protected by human rights legislation. It could enable malicious employers to silently discriminate based on sexual orientation or pregnancy status for example, with little hope

---

[102] Anderson & Jiang, *supra* note 3.
[103] Sarah Frier, "Instagram Looks Like Facebook's Best Hope" (10 April 2018), online: *Bloomberg Businessweek* <www.bloomberg.com/news/features/2018-04-10/instagram-looks-like-facebook-s-best-hope>
[104] Leo Benedictus, "Snapchat: the self-destructing message app that's becoming a phenomenon" (26 June 2013), online: *The Guardian* <www.theguardian.com/technology/shortcuts/2013/jun/26/snapchat-self-destructing-message-app-phenomenon>. Instagram has also implemented a somewhat similar feature which enables users to post to their "Stories. See "Stories," online: *Instagram* <about.instagram.com/features/stories>.
[105] Niloufer Selvadurai, "Not Just a Face in the Crowd: Addressing the Intrusive Potential of the Online Application of Face Recognition Technologies" (2015) 23:3 Int'l JL & Info Tech 187.
[106] *Ibid* at 5.

of detection. On the other hand, a general lack of privacy law literacy could result in a number of well-intentioned employers being unaware of their legislative requirements. One could reasonably envision the average person thinking there is nothing legally wrong with viewing information that is publicly available through a simple google search; if the individual did not want the information out there, they could set their account settings to private. Many are likely unaware that even viewing personal information can constitute collecting information under privacy legislation. This practical lack of safeguards is reflected in public perception of how likely their social media will be used by third parties in spite of legislation: "88% of Canadians are at least somewhat concerned about how companies and organizations might use information available about them online to make decisions about them, such as for a job, an insurance claim or health coverage."[107]

Furthermore, as noted by the BC Privacy Commissioner, personal information online can be inaccurate or outdated, and individuals conducting a search may not select the correct person's profile or it could be a fraudulent account.[108] Although the legislation obligates companies to keep information about individuals accurate, the issues of enforcement and detection would equally apply in this scenario.

Potential Improvements

It is clear that privacy legislation needs to better reflect the societal dependence and importance placed on social media. However, as noted in *R v Connor*, "Privacy can never be absolute. It must be balanced against legitimate societal needs."[109] Even if we recognize that individual's do not fully appreciate what they consent to, we must still respect individual autonomy and freedom for each person to make the decision whether to engage with social media or not. Additionally, overly stringent regulations could easily render social media's business model ineffective and interfere with their proprietary rights to conduct business as they see fit.

General Solutions

One general means of improvement is greater consent requirements. This is already a proposed amendment to *PIPEDA* under Bill C-11,[110] which draws Canada closer to the consent requirements of the EU *General Data Protection Regulation* ("*GDPR*"). Under the new legislation, in order for consent to be valid, the organization must provide "the individual with the following information in plain language:"

> a) the purposes for the collection, use or disclosure of the personal information determined by the organization and recorded under subsection 12(3) or (4);

---

[107] *Survey on Privacy-Related Issues*, *supra* note 4.
[108] *Conducting Background Checks*, *supra* note 47 at 1.
[109] [1995] 4 SCR 411 at para 117.
[110] Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, 2nd Sess, 43rd Parl, 2020 (first reading, 17 Nov 2020).

b) the way in which the personal information is to be collected, used or disclosed;
c) any reasonably foreseeable consequences of the collection, use or disclosure of the personal information;
d) the specific type of personal information that is to be collected, used or disclosed; and
e) the names of any third parties or types of third parties to which the organization may disclose the personal information.[111]

One potential drawback of improved consent however, is if social media accounts are required to provide more meaningful consent, it may only lead to increased consent fatigue and further distance consumers from engaging with their privacy rights. There is also a danger that social media sites might bombard accounts with consent notices with the very realistic chance that most would just consent to avoid the hassle. Again, this solution also fails to address the inadequacies of a consent-based model in the social media context to begin with.

Bill C-11 additionally proposes some factors to consider when determining what is appropriate in the circumstances:

a) the sensitivity of the personal information;
b) whether the purposes represent legitimate business needs of the organization;
c) the effectiveness of the collection, use or disclosure in meeting the organization's legitimate business needs;
d) whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and
e) whether the individual's loss of privacy is proportionate to the benefits in light of any measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual.[112]

While these amendments appear as though they may aid in balancing the power dynamics between consumers and service providers, they once again fail to take into account the fact that the social media businesses model is inextricably at odds with increased privacy. For example, the very contractual premise of a site like Facebook is to exchange your personal information for the use of the app. Under s. 12(3)(e), this transaction would arguably never be proportionate, so it fails to provide meaningful nuance to the consideration of appropriate use of personal information on social media. It is therefore difficult to imagine that these additional considerations will render any fruitful change.

Another means to more generally ensure compliance is to broaden the powers of the Privacy Commissioners. Particularly when combatting dominant, multinational companies like Facebook, it would be useful for the Commissioner to have broader powers to issue fines rather than be forced to appeal to federal courts for enforcement. Currently, under BC legislation, companies can only be fined up to $100,000 which would be a drop in the bucket for these companies, while *PIPEDA* currently does not impose any fines for contravention of the Act, merely damages. Bill C-11 addresses this by establishing a Personal Information and Data

[111] *Ibid.*
[112] *Ibid* s 12(2).

Protection Tribunal which can impose penalties by recommendation of the Commissioner.[113] The amendments would also establish a penalty for contravention of the Act, which would be the higher of either $10,000 or "3% of the organization's gross global revenue"[114] This would bring Canada more in line with *GDPR* which allows for fines of up to four percent of global revenues.[115] While this would not resolve the issue of extraterritorial enforcement, with more countries increasing their pressure on social media companies, it may encourage them to take a more proactive approach in addressing their privacy concerns.

Responsive Measures – Improving Internet and Privacy Literacy

In 2018, the Privacy Commissioners across Canada collectively created publicly accessible lesson plans for teachers to inform students on the importance of privacy, and the privacy implications of social media in particular.[116] The plans are divided into two categories that target grades six to nine, and grades nine to twelve. These lesson plans are crucial and should be implemented into BC school curriculum. Currently, the earliest consideration of the intersections of media and privacy is only required by grade eight.[117] The curriculum should be amended to implement the privacy commissioner lesson plans in grade six.

One challenge of literacy is that it is difficult to disseminate information without the easy access point afforded to minors in school. Therefore, in addition to learning about privacy themselves, children could potentially be used as access points to help educate their network at home, perhaps by sending them home with pamphlets to share with their parents and grandparents. Additional outreach opportunities should also be explored to educate employers on their responsibilities and limitations of using personal information found through social media.

Responsive Measures – De-Indexing, Protecting Minors, and No-Go Zones

Given the lack of adequate means to fully resolve issues of consent without infringing individual autonomy and the proprietary interests of businesses, it is crucial that privacy legislation acknowledges and responds to the fact that personal information is a google-search away contrary to individuals' wishes and is being used in ways that contradict the legislation with limited opportunities for recourse. A crucial means to achieve this lies in the right to be forgotten and de-indexing. There is some debate over whether the right to be forgotten should be limited to de-indexing information so that it cannot appear on search results, or should encompass a broader right to completely erase information as is applied under the *GDPR*.[118]

---

[113] *Ibid* s 93(1).
[114] *Ibid,* s 94(4).
[115] "Two privacy commissioners found AggregateIQ broke privacy laws — but they can't do much about it," (29 November 2019) online: *Canadian Broadcasting Corporation* <www.cbc.ca/radio/day6/amazon-workplace-injuries-enforcing-privacy-laws-photographing-climate-change-hockey-in-north-korea-more-1.5376837/two-privacy-commissioners-found-aggregateiq-broke-privacy-laws-but-they-can-t-do-much-about-it-1.5376847>.
[116] Office of the Information & Privacy Commissioner for British Columbia, *Lesson Plans* (OIPC), online: <https://www.oipc.bc.ca/resources/lesson-plans>.
[117] Government of British Columbia, *Applied Design, Skills, and Technologies 8* (Ministry of Education, June 2016), online: <https://curriculum.gov.bc.ca/curriculum/adst/8/core>.
[118] Andrea Slane, "Information Brokers, Fairness, and Privacy in Publicly Accessible Information" 2018 4-1 *Canadian Journal of Comparative and Contemporary Law* 249.

While the right to be forgotten is a complex issue that far exceeds the scope of this paper, in the very least, individuals should be able to de-index their information in order to protect against improper scraping. What good is it if Facebook removes your data if it is still a Google search away? This is particularly clear cut in the case of protecting more vulnerable populations. The ability to withdraw consent and de-index should unquestionably be a right for minors. In the draft recommendation on online reputation, the OPC highlighted the particular vulnerability of children and suggested, "in the case of information provided to an organization or otherwise posted by youth about themselves, the right to removal should be as close to absolute as possible, and unfettered by any contractual limitations." [119] This would respect a minors autonomy to post as they wish while simultaneously accommodating the reality that most children do not comprehend the implications of what they post or how their information may be used against them.

The Commissioner also recommended Parliament "provid[e] youth with some ability, upon reaching the age of majority, to request and obtain removal of online information posted about them by their parents or guardians who until then had substitute decision-making power."[120] I would argue this should not depend on the age of majority but rather the age upon which a mature minor seeks to assert control over their own privacy. I see no justification for applying a different standard in this context; if a minor is deemed to be of capacity to make their own privacy decisions, then that should apply in all circumstances. Beyond the dignity afforded to minors being able to take control of their own online presence, embarrassing online content could materially impact a young person before they reach the age of majority as they begin to navigate first jobs and university applications. As the Commissioner noted, "[s]uch an ability will, of course, need to be crafted in such a way as to be practical and respect the expressive rights of the parent."[121] While the Commissioner did not expand on this, I would think the particular vulnerability of minors and the dependence they have on guardians to act in their best interests would justify such a limitation on the guardian's expressive rights.

An Ontario White Paper took their recommendations a step further and suggested amendments to their legislation's version of appropriate collection to explicitly exclude "monitoring or profiling of an individual under the age of 16 for the purposes of influencing the individual's behaviour or decisions," as well as "purposes that are known to cause, or are likely to cause, significant harm to the individual or groups of individuals."[122] The Privacy Commissioner of Ontario supported the creation of these no-go zones so long as the exception of targeting minors under 16 did not extend to "educational initiatives that actually benefit children and youth by promoting positive behavioural changes (for example, adopting healthier food choices or engaging in more physical activity), particularly in cases where parental consent has been obtained for such a purpose."[123]

---

[119] *Draft OPC Position on Online Reputation*, *supra* note 89.
[120] *Ibid*.
[121] *Ibid*.
[122] Ontario Government, *Modernizing Privacy in Ontario*, (17 June 2021), online (pdf): <www.ontariocanada.com/registry/showAttachment.do?postingId=37468&attachmentId=49462>.
[123] Information and Privacy Commissioner of Ontario, *IPC Comments on the Ontario Government's White Paper on Modernizing Privacy in Ontario* (Toronto: IPC, September 2021), online (pdf): <www.ipc.on.ca/wp-content/uploads/2021/09/2021-09-03-ipc-comments-on-gov-white-paper_modernizing-privacy-in-ontario.pdf>.

Finally, it is a general requirement that privacy legislation must obtain consent prior to collection, which, in the case of minors who are incapable of exercising their statutory rights, would require parental consent. I believe the legislation should be amended to make it a specific contravention of the Act to obtain information of a child under 13 without the consent of their parent to bring the legislation explicitly in line with our understandings of the capacity of children to consent.[124] Guidance can be taken from the failures of the American application of the *Children's Online Privacy Protection Act*, which has not held social media organizations accountable for the underage minors on their sites even though this violates both the legislation and their own terms and conditions.[125] Effectively, by excluding those under 13 from the sites, these organizations have circumvented the requirements of the legislation even though it is universally accepted that children nonetheless persist in using social media.[126] Therefore, greater measures should be adopted to hold social media organizations accountable for verifying its users' ages by imposing greater responsibility on organizations when they have active knowledge or ought to have known a user was underage.

Conclusion

Although privacy legislation in theory should impose strict restrictions on social media sites to gain informed consent from users before collecting or disclosing information and prevent third party organizations from using your public online content without consent or a legitimate employment purpose, the reality is that privacy legislation is ill-equipped to regulate the privacy interests at stake on social media sites. Privacy law particularly fails to account for the ways in which societal behaviours impact individual choice in which sites they use and what information they make publicly available. Society has become increasingly desensitized to mass information sharing platforms and the blending private and public domains on social media, while it simultaneously seems to be more ambivalent towards those who seek to afford themselves some protection of their privacy online. Given that orders against the social media platforms have repeatedly gone unenforced, and scraping violations are often undetected, it is no wonder that individuals feel that they cannot expect to have any privacy online.

While improved consent and greater Commissioner powers to issue fines may help move privacy law in the right direction, it does not address the inherent limitations of the legislation due to societal behaviour and social media business models. Therefore, the best means to address these concerns are by improving privacy and internet literacy, ensuring the right for individuals to withdraw their consent and de-index, and provide vulnerable minors with greater control over their online content once they are of age to enforce their privacy rights.

---

[124] See Office of the Privacy Commissioner of Canada, *Guidelines for obtaining meaningful consent*, revised 13 August 2021 (Gatineau: OPC, May 2018), online: <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.

[125] Shannon Finnegan, "How Facebook Beat the Children's Online Privacy Protection Act: A Look into the Continued Ineffectiveness of COPPA and How to Hold Social Media Sites Accountable in the Future" (9 January 2020) 50 *Seton Hall L. Rev* 827 (2019-2020).

[126] *Ibid* at 828; "Continuing to Make Instagram Safer," *supra* note 79.

LEGISLATION

Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, 2nd Sess, 43rd Parl, 2020 (first reading, 17 Nov 2020).

Children's Online Privacy Protection Act, 1998, 15 USC 16501-6505.

Freedom of Information and Protection of Privacy Act [RSBC 1996] c 165.

Organizations in the Province of British Columbia Exemption Order, SOR/2004-220.

Personal Information Protection Act, SBC 2003, c 63.

Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

Personal Information Protection Act Regulations, BC Reg 473/2003

JURISPRUDENCE

Google Inc. v Equustek Solutions Inc, 2017 SCC 34.

Google LLC v Equustek Sols Inc, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017)

Investigation Report No P-19-01, 2019 BCIPC 7

Morgaurd Investments Ltd v De Savoye, [1990] 3 SCR 1077 at 1095, [1990] SCJ No 135.

Order P17-03, 2017 BCIPC 38.

Order P20-05, 2020 BCIPC 33.

Order P21-01, 2021 BCIPC 06.

PIPEDA Report of Findings No 2019-002, [2019] CPCSF No 2, [2019] SCCPVPC no 2 (OPC).

R v Jarvis, 2019 SCC 20.

SECONDARY MATERIALS: ARTICLES

Aleecia M. McDonald & Lorrie Faith Cranor, "The Cost of Reading Privacy Policies" (2008) 4:3 ISJLP 543.

Andrea Slane, "Information Brokers, Fairness, and Privacy in Publicly Accessible Information" 2018 4-1 *Canadian Journal of Comparative and Contemporary Law* 249.

Antika Gupta, "*Google v Equustek*: An Attempt to Domestically Govern a Global Resource" (16 October 2017), online: *The Court* <www.thecourt.ca/google-v-equustek-an-attempt-to-domestically-govern-a-global-resource/>.

Bogdan Batrinca & Philip C. Treleaven, "Social media analytics: a survey of techniques, tools and platforms" (26 July 2014, *AI & Soc* 30, 89-116 (2015).

Carsten Schwemmer & Sandra Ziewiecki, "Social Media Sellout: The Increasing Role of Product Promotion on YouTube" (14 August 2018) 4:3 Social Media + Society.

"Continuing to Make Instagram Safer for the Youngest Members of Our Community" (17 March 2021), online: *Instagram*, <https://about.instagram.com/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community>.

"CR Survey: 7.5 Million Facebook Users are Under the Age of 13, Violating the Site's Terms" (May 10, 2011) Consumer Reports, online: <https://www.consumerreports.org/media-room/press-releases/2011/05/cr-survey-75-million-facebook-users-are-under-the-age-of-13-violating-the-sites-terms-/>.

"Creator Fund," online: *TikTok* <https://www.tiktok.com/creators/creator-portal/en-us/getting-paid-to-create/creator-fund/>.

Deepa Seetharaman, Jeff Horwitz & Justin Scheck, "Facebook Says AI Will Clean Up the Platform. Its Own Engineers Have Doubts." (17 October 2021), online: *The Wall Street Journal* <https://www.wsj.com/articles/facebook-ai-enforce-rules-engineers-doubtful-artificial-intelligence-11634338184>.

Fred H. Cate, Peter Cullen & Viktor Mayer Schonberger, "Data Protection Principles for the 21st Century" (2013). *Books by Maurer Faculty*. 23 Mauer School of Law: Indiana University. <www.repository.law.indiana.edu/facbooks/23?utm_source=www.repository.law.indiana.edu%2Ffacbooks%2F23&utm_medium=PDF&utm_campaign=PDFCoverPages>.

Hanbyul Choi, Johnghwa Park & Yoonhyuk Jung, "The role of privacy fatigue in online privacy behaviour" *Computers in Human Behaviour*, vol 81, April 2018, p 42-51.

"Investing $1 Billion in Creators" (14 July 2021), online: *Meta* <about.fb.com/news/2021/07/investing-1-billion-dollars-in-creators/>.

Kate Murphy, "We Want Privacy but Can't Stop Sharing" (Oct 4, 2014), online: *The New York Times* <www.nytimes.com/2014/10/05/sunday-review/we-want-privacy-but-cant-stop-sharing.html>.

Leo Benedictus, "Snapchat: the self-destructing message app that's becoming a phenomenon" (26 June 2013), online: *The Guardian* <www.theguardian.com/technology/shortcuts/2013/jun/26/snapchat-self-destructing-message-app-phenomenon>.

Matthew Rosenberg & Gabriel J.X. Dance, "'You Are the Product': Targeted by Cambridge Analytica on Facebook" (8 April 2018), online: *The New York Times* <www.nytimes.com/2018/04/08/us/facebook-users-data-harvested-cambridge-analytica.html> .

Monica Anderson and Jingjing Jiang, "Teens, Social Media and Technology 2018" (31 May 2018), online: *Pew Research Center* <https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/>.

Niloufer Selvadurai, "Not Just a Face in the Crowd: Addressing the Intrusive Potential of the Online Application of Face Recognition Technologies" (2015) 23:3 Int'l JL & Info Tech 187.

Pavni Diwanji, "How Do We Know Someone Is Old Enough to Use Our Apps?" (27 July 2021), online: *Meta* <about.fb.com/news/2021/07/age-verification/>

Ramona Pringle, "Youth is no defence when it comes to shameful online posts," (16 June 2017), online: *CBC* <www.cbc.ca/news/opinion/youth-is-no-defence-when-it-comes-to-shameful-online-posts-1.4160070>.

Shannon Finnegan, "How Facebook Beat the Children's Online Privacy Protection Act: A Look into the Continued Ineffectiveness of COPPA and How to Hold Social Media Sites Accountable in the Future" (9 January 2020) 50 *Seton Hall L. Rev* 827 (2019-2020).

Sonia Livingstone, Mariya Stoilova, & Rishita Nandagiri, "Talking to children about data and privacy online: research methodology" (6 September 2018) online: *London School of Economics and Political Science, Department of Media and Communications* <blogs.lse.ac.uk/parenting4digitalfuture/2018/09/06/theorising-privacy-how-do-and-how-should-children-know/>.

"Stories," online: *Instagram* <about.instagram.com/features/stories>.

"The strategic privacy priorities," last modified 14 December 2018, online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/about-the-opc/opc-strategic-privacy-priorities/the-strategic-privacy-priorities/#reputation>.

"Two privacy commissioners found AggregateIQ broke privacy laws — but they can't do much about it," (29 November 2019) online: *Canadian Broadcasting Corporation* <www.cbc.ca/radio/day6/amazon-workplace-injuries-enforcing-privacy-laws-photographing-climate-change-hockey-in-north-korea-more-1.5376837/two-privacy-commissioners-found-aggregateiq-broke-privacy-laws-but-they-can-t-do-much-about-it-1.5376847>.

"YouTube Partner Program overview & eligibility," online: *YouTube Help* <support.google.com/youtube/answer/72851?hl=en>.

SECONDARY MATERIALS: GOVERNMENT DOCUMENTS

Information and Privacy Commissioner of Ontario, *IPC Comments on the Ontario Government's White Paper on Modernizing Privacy in Ontario* (Toronto: IPC, September 2021), online (pdf): <www.ipc.on.ca/wp-content/uploads/2021/09/2021-09-03-ipc-comments-on-gov-white-paper_modernizing-privacy-in-ontario.pdf>.

Office of the Privacy Commissioner of Canada, *Certificate of nomination of Daniel Therrien to the position of Privacy Commissioner Issue Sheets*, (OPC), online: <www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/ethi_20210621/is_ethi_20210621/#toc18>.

Office of the Information & Privacy Commissioner for British Columbia, *Conducting Social Media Background Checks,* May 2017 update (Victoria: OIPC).

Office of the Privacy Commissioner of Canada, *Draft OPC Position on Online Reputation*, last modified 26 January 2018, (Gatineau: OPC), online: <www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/pos_or_201801/#heading-0-0-5>.

Office of the Privacy Commissioner of Canada, *Guidelines for obtaining meaningful consent*, revised 13 August 2021 (Gatineau: OPC, May 2018), online: <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.

Office of the Privacy Commissioner of Canada, *Notice of Application with the Federal Court against Facebook, Inc.*, 6 February, 2020, (Gatineau: OPC), online: < https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-complaints-and-enforcement-process/court_p/na_fb_20200206/>.

Office of the Privacy Commissioner of Canada, *PIPEDA Report of Findings #2009-008*, (OPC, 16 July 2009), online: <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-008/>.

Office of the Privacy Commissioner of Canada, *2020-21 Survey of Canadians on Privacy-Related Issues*, Catalogue No IP54-109/2021E-PDF (Gatineau: OPC, 10 March 2021), online: <www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/por_2020-21_ca/#fig01>.

Ontario Government, *Modernizing Privacy in Ontario*, (17 June 2021), online (pdf): <www.ontariocanada.com/registry/showAttachment.do?postingId=37468&attachmentId=49462>.

Statistics Canada, *Canadians' assessments of social media in their lives*, by Christopher Schimmele, Jonathan Fonberg & Grant Schellenberg, in *Economic and Social Reports*, last modified 26 October 2021, (Ottawa: Statistics Canada, 24 March 2021), online: <www150.statcan.gc.ca/n1/pub/36-28-0001/2021003/article/00004-eng.htm>.

Statistics Canada, Table 22-10-0143-01 Smartphone personal use and selected habits by gender and age group, (Ottawa: Statistics Canada, June 22, 2021), online: <https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=2210014301&pickMembers%5B0%5D=3.1&pickMembers%5B1%5D=4.2&cubeTimeFrame.startYear=2018&cubeTimeFrame.endYear=2020&referencePeriods=20180101%2C20200101>.