An Unfair Game of Virtual Hide-and-Go-Seek: The Passive Collection of Children's Information Online

Submitted By:

Andrea Korajlija
J.D. Candidate, 2021
Faculty of Law, Common Law Section
University of Ottawa

Submitted To:

The Interdisciplinary Research Laboratory on the Rights of the Child (IRLRC)
2019-2020 Essay Competition

15 May 2020

Table of Contents

I dedicate this paper to Ruby Kerr, so that all children like her may flourish in the digitalized world, as her father would have wanted.

1 … 2 … 3
Let’s play a game of virtual hide-and-go seek
4 … 5 … 6
The children will hide
7 … 8 … 9
And we will seek
10
Ready or not, here we come

I. NO HIDING, ALL SEEKING

Today, there is no place for a child to hide online – they have a digital footprint before they can walk and an audience before they can see. But there are many places for us to seek – from conception to birth and subsequent birthdays, we see the child on Facebook, Instagram, YouTube, blogs, and the like. As a child grows, so does the myriad of information divulged by their parents. Intimate memories are captured through their online activities, adored by relatives and friends, observed by strangers, and exploited by others. Data on children enters this world and develops much faster than they do, and our legal system is failing to keep up with the pace.

In this paper, I examine the regulatory deficiencies surrounding children's online privacy. Specifically, I assess how the passive collection of children's information through their parents is permitted under the current legislation. I examine two online activities of parents that jeopardize their children's privacy: (1) "sharenting" on social media platforms; and (2) the use of pregnancy and parenting mobile applications. I outline the consequences children face because of this unconsented passive collection of their information enabled by their parents' technology use. Lastly, I call for more stringent regulation. We need legislation that explicitly differentiates children's privacy interests and offers specific safeguards for them to preserve their digital identity and overall safety.

II. THE PARADOXICAL PARENT: PROTECTOR AND DILUTER

The benefits of technology are palpable and alluring, but speed, connectivity, and accessibility to information has swept us off our feet and left us blindsided to the consequences. Investigating the consequences is more important than ever as we now

have entire generations growing up in the digitalized world for the first time in history. This paper examines one significant consequence – the internet's erosion of children's privacy. Privacy, a vehicle of intimacy denoting the boundaries of our social relationships,[1] is necessary for self-determination, self-development, and security of the person.[2] Yet, children born as "digital citizens" are forced to navigate fast-paced, hyperconnected relations archived in the internet's apparently infinite capacity. The lack of privacy in the digitalized world can lead children to commercial and sexual exploitation, surveillance, cyberbullying, and irreparable damage of reputation.[3] As children are uniquely positioned in the digitalized world – with the most to gain, and the most to lose – we must ensure that their legal protections remain effective in this new environment.

Currently, Canada's privacy legislation does not explicitly recognize children's privacy rights. The *Personal Information Protection and Electronic Documents Act* (PIPEDA),[4] overseen by the Office of the Privacy Commissioner of Canada, applies to private-sector organizations in Canada that collect, use, or disclose personal information in the course of commercial activity. Absent any differentiation between child and adult, all provisions in the Act are meant to equally protect both cohorts.

However, to account for children's difficulties in fully appreciating the dangers stemming from their online activities, the Act permits parents to intervene. Parents can ensure their children's online activities are conducive to safe internet use and determine the extent of their child's online exposure by providing substitute consent. Under Clause

[1] Jeffrey H. Reiman, "Privacy, Intimacy, and Personhood" (1976) 6:1 Philosophy & Public Affairs 26; James Rachels, "Why Privacy is Important" (1975) 4:4 Philosophy & Public Affairs 323.
[2] Eric Barendt, *Privacy* (London: Routledge, 2001).
[3] Eva Lievens, *Protecting Children in the Digital Era: The Use of Alternative Regulatory Instrument* (Leiden, Boston: Marthinus Nijhoff Publishers, 2010) at 52-57.
[4] *Personal Information Protection and Electronic Documents Act,* SC 2000 c 5 [PIPEDA].

4.3 of Schedule 1 to PIPEDA, "the knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate."[5] As a general rule for anyone under the age of 13, consent must be obtained from their parents or guardians.[6] Specifically, in circumstances where the online services are *directed at children* and obtaining information *from children*, the parent has legal authority to consent on the child's behalf.[7]

The narrowly constructed language of the legislation fails to capture instances where information *about children* is gathered *indirectly*. Consequently, privacy protections are only triggered when information flows from the child to the organizations. Privacy protections are not triggered when information about children flows through an external channel – like their parents – to organizations. The gap in the legislation is troublesome because parents are a loophole for a significant amount of children's information to end up in the hands of private organizations and other potential predators.

Interestingly, despite their ability to provide substitute consent for children, only 17% of parents in a 2018 Canadian survey asked their child for their consent prior to uploading content about the child online.[8] By depicting parents as the gatekeepers of children's privacy, the legislation has ignored the idea of parents as the diluters of children's privacy. Information overlap naturally exists between a parent and their child. However, PIPEDA fails to explicitly recognize the joint interest a parent and child have in

[5] PIPEDA *supra* note 4, c 4.3 of Schedule 1.
[6] Privacy Commissioner of Canada, "Guidelines for obtaining meaningful consent" (last modified 24 May 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.
[7] PIPEDA *supra* note 4, s. 6.1.
[8] Kara Brisson-Boivin, "The Digital Well-Being of Canadian Families" (2018) MediaSmarts, online (pdf): <https://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/digital-canadian-families.pdf>.

the parent's online activities. Instead, parents are given unilateral decision-making power over their child's privacy.

Ultimately, parents are consenting to the collection, storage, and use of their own data without understanding how it affects their children. Perhaps parents are unaware or simply ignorant to the consequences of their online activities. When asked, only 11% of Canadian parents indicated that they regret sharing content related to their children.[9] To truly protect children, the law must also account for parents' difficulties in fully appreciating the dangers their own online activities create for children. As such, the passive collection of children's information through their parents' online activities needs to be addressed in our privacy legislation.

III. HOW CHILDREN'S ONLINE DATA IS CONCEIVED

This paper focuses on two ways in which parents make consensual disclosures of their own information online that directly affects their children. Parents are facilitating the accumulation of a significant amount of children's information by: (1) oversharing on social media platforms to capture their children's personal moments and milestones; and (2) using pregnancy and parenting mobile applications to track their children's progress.

1. Parents are engaged in online "sharenting" of their children

The problem of parents posting content related to their children online has become so pervasive that it has been coined "sharenting" – "the practice of parents regularly using social media to communicate a lot of detailed information about their children."[10] The

[9] MediaSmart *supra* note 8.
[10] "Sharenting" (last modified 20 August 2013), online: *Collins Dictionary* <https://www.collinsdictionary.com/submission/11762/Sharenting>; Leah A. Plunkett, *Sharenthood: Why We Should Think before We Talk about Our Kids Online* (Cambridge: MIT Press, 2019).

sharenting commonly starts when parents to-be announce their pregnancy through social media. Friends and followers get to peek into the new little life before it arrives: ultrasound photos show the fetus, gender reveal photos confirm the sex of the baby, photos of the nursery depict the family's evolving home. Friends and followers become spectators as the sharenting continues indefinitely. In a 2018 Canadian survey by MediaSmart, 73% of parents stated that they sometimes share photos, videos, or blog about their children. The numbers align with international trends; in the U.K., a 2016 survey found that parents post nearly 1500 photos online by a child's fifth birthday.[11] More information on children will inevitably find its way online as parents admit they struggle to identify where their child's identity ends and theirs begins.[12]

Parents willingly disclose their children's information to stay connected, validated, and rewarded. In some cases, that reward can be financial, such as when parents establish their vlogging and blogging careers by posting content related to their children online. Connection, validation, and reward result in positive stimuli that induce parents to continue exposing personal information in the public domain.[13] For example, think of Charlie biting his brother's finger.[14] The video has over 873 million views online. Ten years later, when Charlie can speak, he says people at school would talk about the video a lot.[15] In a follow-up interview, Charlie's father said he feels great about posting a video that has

[11] Nominet, "Share with Care" (2016), online: <https://media.nominet.uk/wp-content/uploads/2016/09/Nominet-Share-with-Care-2016-Infographic.pdf>.
[12] Frederike Lichtenstein et al, "Growing up on YouTube – How family vloggers are establishing their children's digital footprints for them" (23 October 2007), online: *New Media & Digital Culture M.A, University of Amsterdam* < https://mastersofmedia.hum.uva.nl/blog/2017/10/23/growing-up-on-youtube-how-family-vloggers-are-establishing-their-childrens-digital-footprints-for-them/>.
[13] Stacey B. Steinberg, "Sharenting: Children's Privacy in the Age of Social Media" (2017) 66 Emory LJ 839 at 846.
[14] HDCYT, "Charlie bit my finger – again !" (22 May 2007), online (video): *YouTube* <https://www.youtube.com/watch?v=_OBlgSz8sSM>.
[15] StoryTrender, "Charlie Bit My Finger 10 Year Anniversary" (21 May 2017) at 00h:00m:35s, online (video): *YouTube* <https://www.youtube.com/watch?v=bOuu_3-gAn0>.

made an impact and influenced people's lives.[16] Such statements embody the positive stimuli described above in full effect. The video is projected to be worth a million pounds and has taken the family all around the world to film advertisements in America and meet many influential people.[17] Ever since, the family has continued to build their YouTube channel and online presence. Charlie's mother indicated "a lot of people liked seeing Harry and Charlie growing up and following the family story. They knew [she] was pregnant with Jasper and now they're watching him grow up."[18] One cute and innocuous video has snowballed into the regular online documentation of family matters.

The fame, fortune, and fun memories come at the expense of their children's privacy. Although absent any malice on behalf of the parents, their online activity eliminated their children's choice to privacy. Charlie and his brothers are not alone – many families have established successful online-based careers by recording their children. In the U.S. alone, there are about 4.2 million parents who read and write blogs.[19] On YouTube, family channels have accumulated millions of subscribers.[20] While blogging or vlogging, parents are incentivized to continue generating more content by significant sponsorship opportunities and advertising revenues.[21] Introducing financial incentives for parents to disclose children's information online makes it even more challenging for children to preserve their privacy. In the case of Charlie and children alike, "the question of agency or control becomes even more important when the legacy or history of that

[16] *Ibid.*
[17] *Ibid.*
[18] David Masters, "Two British brothers have made internet history by clocking up 250 Million YouTube hits" (20 July 2010), online: *The Sun* <https://en.wikipedia.org/wiki/Charlie_Bit_My_Finger#cite_note-Masters-8>.
[19] Alicia Blum-Ross & Sonia Livingstone, "'Sharenting", parenting blogging, and the boundaries of the digital self" (2017 April 17) 15:2 Intl J of Media and Culture 110 at 111.
[20] Feedspot, "100 Family Youtube Channels By Family Youtubers" (last updated May 10, 2020), online: <https://blog.feedspot.com/family_youtube_channels/>.
[21] *Supra* note 19 at 113.

identity may be entirely inescapable."[22] The lack of children's privacy rights is being capitalized on by their own parents for the sake of popularity and monetary gains.

Regardless of whether the sharenting is a professional or personal pursuit, children are left to bear the consequences of their parents' online activities. Although parents have historically always shared information on their children – whether through newspaper postings on birthdays or photos tucked into wallets for display – the means, scope, and extent of sharing today is much greater than ever before, as are the dangers. This paper touches on three dangers children could face as a result of sharenting: (1) bullying; (2) sexual exploitation; and (3) reputational harm.

Through sharenting, parents are unknowingly increasing their child's risk of being bullied. Research conducted with focus groups aged 12-14 demonstrated that children find their parents' online activity reckless at times.[23] Children complained about the lack of precautionary privacy measures on their parents' social media accounts. Concerns of bullying emanated through the children's responses when asked about the potential consequences of their parents' sharenting. Children grasp the widespread visibility and dissemination of online content. The focus groups emphasized the importance of immediate removal of embarrassing content from parents' accounts. However, the inherent power imbalance in the parent-child relationship can inhibit a child from removing the content quickly. Some children noted taking action themselves, by logging on to their parents' devices and accounts to remove images or videos, before it was "too late."[24] As

[22] Tama Leaver, "Born Digital? Presence, Privacy and Intimate Surveillance" in Hartley, John & W. Qu, ed, *Re-Orientation:Translingual Transcultural Transmedia.* (Shanghai: Fudan University Press, 2015) 149 at 151.
[23] Gaëlle Ouvrein & Karen Verswijvelpage, "Sharenting: Parental adoration of public humiliation? A focus group study on adolescents' experiences with sharenting against the background of their own impression management" (2019) 99 Chlidren and Youth Services Review 319 at 321.
[24] *Ibid* at 323.

technology has made bullying easier, faster, widespread, and crueler than ever before,[25] parents should be particularly vigilant about their sharenting habits.

The innocent photo or video of a child posted online portrays much more than them eating, playing, or potty-training. Rather, it is a relic of their appearance, location, and development on the internet – a place where one can never be certain that only friends and family can see. According to a study by the University of Michigan, 51% of parents provided information that could lead to an identification of their child's location at any given time, and 27% shared potentially inappropriate photos.[26] Australia's eSafety Commissioner reports that nearly half of all images found on pedophile image sharing sites are originally posted with a parent's innocent intent on social media and family blogs.[27] The alarming statistics show a clear need for measures to protect children's privacy online, as there is a strong correlation between sharenting and children's safety.

Lastly, a tainted online reputation can follow a child for many years and may be visible to influential figures. The impact can be significant in the child's adolescent stages, when they are establishing and validating a teenage identity.[28] At that stage, the most influential figures in the child's life are their peers – those they wish to be accepted by.[29] As a result, adolescent children actively engage in impression management. They are

---

[25] The Report of the Nova Scotia Task Force on Bullying and Cyberbullying, "Respectful and Responsible Relationships: There's No App for That" (29 February 2012), online: <http://antibullying.novascotia.ca/sites/default/files/Respectful%20and%20Responsible%20Relationships%2C%20There%27s%20no%20App%20for%20That%20-%20Report%20of%20the%20NS%20Task%20Force%20on%20Bullying%20and%20Cyberbullying.pdf>.
[26] C.S. Mott Children's Hospital, "National Poll on Children's Health" (16 March 2015), online: *Parents on Social Media Dislikes of Sharenting* <https://mottpoll.org/sites/default/files/documents/031615_sharenting_0.pdf>.
[27] Lucy Battersby, "Millions of social media photos found on child exploitation sharing sites", *The Sydney Morning Herald* (30 September 2015), online: <https://www.smh.com.au/national/millions-of-social-media-photos-found-on-child-exploitation-sharing-sites-20150929-gjxe55.html>.
[28] Laurence Steinberg, "Puberty, Cognitive transition, Emotional transition, Social transition", online (blog): *Adolescence* <https://psychology.jrank.org/pages/14/Adolescence.html>.
[29] *Supra* note 23 at 320.

hyper-sensitive towards what they do and do not share within their social circles.[30] As if navigating teenage years was not difficult enough, the Internet has created an additional domain for today's adolescent children to oversee. According to the Impression Management Theory, one's online reputation is determined by their own expressions, as well as those of others.[31] Regrettably for these vulnerable adolescents, approximately 56% of parents share potentially embarrassing information about their children online.[32] Harm to reputation from sharenting can extend beyond the adolescent stages and into adulthood, where potential employers may gain insights into private matters.[33] Since parents hold the pen on a child's digital story for so many years, it is becoming increasingly challenging for them to author their own online reputation.

2. Parents use mobile applications to maneuver pregnancy and parenthood

Beyond sharenting on social media platforms, parents using mobile applications also discretely funnels children's information to the online world. Specifically, pregnancy and parenting mobile apps are effective at extracting detailed information on a child throughout their early stages of life. Pregnancy apps provide parents an accessible and easy method of logging information such as "conception date, weight, number of kicks in the womb, possible names, cultural backgrounds, heart rate, diet before conception, parents' thoughts, family ties, family medical history, complications during pregnancy, and due date."[34] Upon birth, parenting apps offer a wide range of monitoring for areas such

[30] Danah Boyd, "Why Youth (Heart) Social Networks Sites: The Role of Networked Publics in Teenage Social Life" (2007) Youth, Identity, and Digital Media, David Buckingham, ed., The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning, The MIT Press at 129.
[31] *Supra* note 23 at 321.
[32] *Supra* note 26.
[33] Children's Commission, "Who Knows what about me?" (November 2018), online: <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/11/cco-who-knows-what-about-me.pdf> at 14.
[34] Veronica Barassi, "BabyVeillance? Expecting Parents, Online Surveillance and the Cultural Specificity of Pregnancy Apps" (2017) 1:10 Social Media + Society at 2.

as infant feeding, sleeping, growth and development, and childcare.[35] Both types of applications typically allow users to connect to their social media accounts and contribute to discussion forums.

Pregnancy and parenting apps have become pivotal tools for modern-day families. The users, often women, seek answers to the uncertainties of caring for a newborn, and create connections with others to help cope with the loneliness and social isolation commonly accompanying childbirth.[36] Some mobile applications in the market have amassed over ten million users and billions of data points.[37] The apps have fostered a large and trusting environment where users do not actively assess the validity of the predictions or consider the security and privacy implications of their use.[38]

Organizations are leveraging this trust and further exploiting it through their ambiguous privacy policies. The privacy policies, meant to inform users on data-handling provide little to no specificity on who has access to the data and what it will be subsequently used for.[39] The users do not have an informed understanding about their data, and consequently lose control over not only their personal identifying information[40] but that of their child as well. The collection, use, and disclosure of the child's information gathered from the parent's activity is typically omitted from the privacy policies of

[35] Deborah Lupton, Sarah Pederson & Garreth M Thomas, "Parenting and Digital Media: From the Early Web to Contemporary Digital Society" 10:8 Sociology Compass 730 at 735.
[36] Deborah Lupton, "The use and value of digital media for information about pregnancy and early motherhood: a focus group study" 16:171 BMC Pregnancy and Childbirth 1.
[37] Drew Harwell, "Is your pregnancy app sharing your intimate data with your boss?" *The Washington Post* (10 April 2019), online: <https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/>.
[38] Deborah Lupton & Sarah Pedersen, "An Australian survey of women's use of pregnancy and parenting apps" 29:4 Women & Birth 368.
[39] *Supra* note 34 at 5.
[40] *Ibid* at 6.

pregnancy and parenting applications.[41] When it is mentioned, the companies are usually carving out a right to use the information. For example, *BabyConnect*, claiming to be the most comprehensive baby tracking application in the Appstore,[42] has a privacy policy that reads:

> This site is not intended for children under the age of 13. We will not knowingly collect personally identifiable information via this site from visitors in this age group. *We do, however, collect information about children and babies from their parents or their caregivers (nannies, baby-sitters, ...).* We ask that our users not provide information about a baby or child without first getting the parents' consent (11 May 2020).

Consequently, the organization can gather information on feedings, nursing, naps, diapers, milestones, pumping, the baby's mood, temperature, what kind of games they are playing, GPS location, pictures, vaccinations, medicines, growth charts, and more. The organization's vague privacy policy, coupled with the current deficiencies in the law, prevent a parent from benefitting from technologies without jeopardizing their children's privacy.

The typical harms of hacking, cybercrime, and the misuse of data affect both adults and children.[43] However, since children are malleable "economic objects,"[44] they are particularly susceptible to targeting by private organizations. The dual role of a child as

---

[41] *Supra* note 34 at 5.
[42] *BabyConnect,* online: <https://www.babyconnect.com>.
[43] Deborah Lupton & Ben Williamson, "The datafied child: The dataveillance of children and implications for their rights" (2017) 19:5 New Media & Society 780 at 787.
[44] Donell Holloway, "Surveillance capitalism and children's data: The Internet of toys and things for children" (2019) 170:1 Media Intl Australia 27 at 28.

data subject and marketing subject makes them extremely valuable.[45] With a children's merchandise market worth hundreds of billions of dollars in the U.S. alone, data brokers are keen on harbouring children's data.[46] Children's data produced by their parents' activity gives data brokers an inlet to create mini-profiles early on, which only continue to grow larger with time.[47] If organizations know and understand children as consumers long before they make their first purchase, it increases the likelihood of manipulation.[48] As organizations openly express a desire to "change people's actual behaviour at scale,"[49] children should be especially protected from their powerful influence.

Detailed, fulsome data accumulation over an entire lifetime is a new phenomenon faced only by those conceived in the digitalized world. The long-term consequences for children are difficult to predict.[50] The uncertain and unknown future applications and integrations of children's data leave us with no assurances.[51] We need legislative change today to protect the children of tomorrow.

IV. SOLUTIONS FOR YOUNG DIGITAL CITIZENS

Canada's response to the deterioration of children's online privacy is lacking. Internationally, several jurisdictions have set strong precedents that could serve as models to enhance children's privacy in Canada. For example, in the U.S. the *Children's Online Privacy Protection Act* (COPPA)[52] is dedicated to protecting children under the

[45] Holloway, *supra* note 44 at 34.
[46] Steinberg, *supra* note 13 at 849.
[47] *Ibid.*
[48] Carly Nyst, "Privacy, Protection of Personal Information and Reputation" (2017) UNICEF Discussion Paper Series: Children's Rights and Business in a Digital World at 11.
[49] *Ibid.*
[50] Holloway, *supra* note 44 at 32.
[51] Gabrielle Berman & Kerry Albright, "Children and the Data Cycle: Rights and Ethics in a Big Data World" (2017) UNICEF Office of Research at 2.
[52] *Children's Online Privacy Protection Rule,* 15 USC 6501-6508 tit 16, c I, sc C.

age of 13 from inappropriate collection of personal information. Pursuant to the *Privacy Rights for California Minors in the Digital World*[53] law, children in California also have the right to request the removal of content or information posted on an operator's website.[54] Similar measures have been adopted in the European Union's *General Data Protection Regulation* (GDPR).[55] Specifically, Article 17 of the GDPR enumerates six grounds under which a data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay. The ability to remove personal content or information, as provided for in California and the European Union, is colloquially known as "the right to be forgotten." The right to be forgotten offers a potential solution to balance the competing interests of parents and their children online, which is currently missing from Canada's privacy regulatory framework.[56]

An effective solution will allow parents to fully use and benefit from today's social media platforms and technological innovations without having to compromise their children's privacy. An effective solution will provide children with tangible recourse while respecting the delicate and intertwined parent-child relationship. To fill the privacy gap currently exposing children to severe consequences, I propose that Canada first enact privacy legislation specific to children – similar to COPPA in the U.S. Within that legislation, children should be afforded the right to be forgotten from content or information generated from: (1) their own online activities; and (2) their parent's online activities. This two-pronged right to be forgotten should be informed by existing family law

[53] *Business and Professions Code*, Division 8. Special Business Regulations [18400 - 22948.25], c 22.1, online: <http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.1.&lawCode=BPC>.
[54] *Ibid.*
[55] EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016,* [2016] PJ, L 119/1.
[56] Stacey Steinberg, "How Europe's 'right to be forgotten' could protect kids' online privacy in the U.S." *The Washington Post* (11 July 2018), online: <https://www.washingtonpost.com/news/parenting/wp/2018/07/11/how-europes-right-to-be-forgotten-could-protect-kids-online-privacy-in-the-u-s/>.

concepts such as the best interests of the child. Further, the legislation should require online service providers passively collecting children's information to provide explicit notice to parents.

1. Enacting privacy legislation specific to children

Through COPPA, the U.S. has granted children's privacy the particular attention that it warrants. Canada should enact legislation similar to COPPA where children's needs, interests, and protection thereof, are clearly spelled out. The scope, definitions, and requirements of COPPA can provide the basic framework for the Canadian legislation. In addition to creating child-specific privacy legislation, the first prong of the proposed right to be forgotten should be based off California's *Privacy Rights for California Minors in the Digital World*.[57] The law mandates, for children with registered accounts, organizations must:

- Allow the child to remove its information from the website servers;
- Provide notice that the child can remove account information and posts from the website servers;
- Provide instructions on how to remove information; and
- Provide notice that the removal may not be completely comprehensive.[58]

The second prong of the right to be forgotten should allow a child, upon the age of majority, to request removal of their online information originally produced by their parents. Without such a right, children will be unable to combat the long-term

[57] *Business and Professions Code*, *supra* note 53.
[58] *Ibid*; Law Offices of Salar Atrizadeh, "Privacy Rights for California Minors" (18 December 2017), online (blog): <https://www.internetlawyer-blog.com/privacy-rights-california-minors/>.

consequences arising from the passive collection of their information through their parent's online activities. The legislature has already provided adequate direction to create such a remedy. Specifically, in creating the child's right to be forgotten from parent-produced content and information, we can draw from family law concepts such as the best interests of the child.

The best interests of the child are codified in Bill C-78,[59] which comes into force on June 1, 2020. Section 16(3) enumerates the factors a court shall consider in determining the best interests of the child, such as the child's needs, given the child's age and stage of development. Moreover, section 16(4) provides a separate list of factors a court will account for when considering family violence. The rationale underpinning each factor in this list is preserving the child's safety – the same concern that emanates from the passive collection of children's information. As such, this list can be particularly helpful in generating a statutorily based right to be forgotten from parent-produced online content. For example, when determining the grounds for the proposed right to be forgotten, the following should be considered: the sensitivity, seriousness and nature of information disclosed; the frequency of disclosure; the size of the audience; the potentially adverse affects on the child; the parent's alternative means of online communication; and the general public interest in the disclosure. By translating existing legal concepts to novel issues faced by children in the digitalized world, we will be able to create efficient and effective solutions.

[59] Bill C-78, *An Act to amend the Divorce Act, the Family Orders and Agreements Enforcement Assistance Act and the Garnishment, Attachment and Pension Diversion Act and to make consequential amendments to another Act*, 1st Sess, 42nd Parl, 2019 (assented to 21 June 2019).

The child's right to be forgotten will have to be constitutionally compliant which may pose challenges because parents have the right to freedom of expression. A right to be forgotten without clear limits lends too much power to the individual's privacy interest over the interests of the public and press to access information.[60] Luckily, the courts have identified and acted on the need to protect children online. In fact, the Supreme Court of Canada has limited long-standing judicial principles to ensure the wellbeing of children.[61] Barring an entire constitutional analysis, the safety and wellbeing of children stands to be a reasonable limitation on the right to freedom of expression because of the dangerous consequences stemming from online activity. Importantly, a child's right to be forgotten was successfully introduced in a U.S. state, where the First Amendment protects freedom of speech.[62] As such, legislating a Canadian child's right to be forgotten with explicit boundaries would likely be constitutionally valid.[63]

Ultimately, the natural informational intersection between parent and child, the inherent power imbalance in the relationship, and the currently permitted passive collection of children's information through their parents, creates an identifiable issue that lends itself to regulation. My proposal for child-specific privacy legislation and a two-pronged right to be forgotten is only a preliminary assessment of the potential solutions that could be viable for children in the digitalized world. A further analysis into the procedural elements of such solutions will have to be conducted.

---

[60] Amy Gajda, "Privacy, Press and the Right to be Forgotten I the United States" (2018) 93:201 Washington L Review 201 at 257.
[61] For example, see *AB v Bragg Communications Inc*, 2012 SCC 46.
[62] James Lee, "SB 568: Does California's Online Eraser Button Protect the Privacy of Minors?" 48:1173 University of California, Daivs 1173 at 1203.
[63] John Bicker et al, "Submission to the Office of the Privacy Commissioner of Canada in Response to the Notice of Consultation and Call for Essays — Online Reputation" (2016) Report for the Office of the Privacy Commissioner, online: <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/submissions-received-for-the-consultation-on-online-reputation/or/sub_or_10/>.

2. Explicitly informing and warning parents of passive collection

To better protect children, parents must be better informed. The child-specific privacy legislation should require online service providers to explicitly outline the collection, use, and disclosure of children's information gathered through their parents' activity. Currently, private organizations are passively collecting large amounts of children's data with little to no mention of it in their privacy policies. The omission exists because the intersection between a parent and child's information is treated indistinguishably. Thus, it is presumed that a parent's express consent regarding their information implicitly extends to the data they divulge about their child. Essentially, this presumption leads to "two-in-one" consent. To obtain "meaningful consent"[64] in these circumstances, organizations need to provide parents with more detailed information.

Privacy policies similar to that of *BabyConnect* insufficiently equip parents to make decisions regarding their children's privacy. Organizations should provide parents with comprehensive information and foreworn them about the passive collection of children's information. Simply stating that "*We do, however, collect information about children and babies from their parents or their caregivers (nannies, baby-sitters, ...)*" does not meet the threshold for meaningful consent. Parents need to know what information about their child is collected, for what purposes it is being collected, used, or disclosed, with whom it is being shared, and what risks of harm exist.[65] Otherwise, parents will continue to unknowingly jeopardize their children in the digitalized world.

[64] Privacy Commissioner of Canada, "Obtaining meaningful consent" (last modified 12 July 2019), online: <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/info_mc/>.
[65] Privacy Commissioner of Canada, "Guidelines for obtaining meaningful consent" (last modified 24 May 2018), online: <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.

Researchers have suggested a "public-health" approach to mitigating the consequences arising from parental disclosures of children's information.[66] Under this approach, best practices would be mainly disseminated to parents through health professionals.[67] Educators, pediatricians, policymakers, and the media would also assist in shaping societal discourse on the issue. While I agree that parental awareness is crucial, I think private organizations have a greater role to play in this process. My proposal aligns with the public-health model but takes it one step further by placing responsibility on the organizations to properly inform parents. If organizations wish to profit from the passive collection of children's data, they should do it with transparency. Parents deserve peace-of-mind when choosing to disclose information, especially when the information is intimate in nature. Parents understanding the implications of their online disclosures is a necessary step to safeguarding children.

V. ACHIEVING A FAIR GAME OF VIRTUAL HIDE-AND-GO-SEEK

Parents have a legal responsibility to safeguard their children online, yet oddly enough, they play a significant role in producing children's online information. The passive collection of information through parents' online activities exposes children to harm that can certainly be felt now and linger indefinitely into the future. To preserve a child's privacy and ensure their safety, Canada needs child-specific privacy legislation. The legislation should include a right to be forgotten similar to California's *Privacy Rights for California Minors in the Digital World*. However, that right to be forgotten should extend further to parent-produced content and information. Additionally, requiring online service providers

[66] Steinberg, *supra* note 13 at 877.
[67] *Ibid* at 878.

to give explicit notice regarding the passive collecting of children's data, will serve to fully inform parents.

The Internet is not forgiving. In Canada, all trust is placed in the hands of the parent to make the right decision for their child – a daunting responsibility. Undoubtedly, there will be situations where the right choice was not made. In addition to explicitly recognizing children's privacy rights, the law must afford children a mechanism to shield themselves from the harmful and long-lasting consequences of their parent's online activities. We need to reform our laws to reflect the uniquely digitalized world of today's children and allow them to play a fair game of virtual hide-and-go-seek.

VI. REFERENCES

Legislation:

Bill C-78, *An Act to amend the Divorce Act, the Family Orders and Agreements Enforcement Assistance Act and the Garnishment, Attachment and Pension Diversion Act and to make consequential amendments to another Act*, 1st Sess, 42nd Parl, 2019 (assented to 21 June 2019).

Business and Professions Code, Division 8. Special Business Regulations [18400 - 22948.25], c 22.1.

Children's Online Privacy Protection Rule, 15 USC 6501-6508 tit 16, c I, sc C.

EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016,* [2016] PJ, L 119/1.

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

Jurisprudence:

AB v Bragg Communications Inc, 2012 SCC 46.

Secondary Materials: Articles

Barassi Veronica, "BabyVeillance? Expecting Parents, Online Surveillance and the Cultural Specificity of Pregnancy Apps" (2017) 1:10 Social Media + Society.

Berman Gabrielle & Albright Kerry, "Children and the Data Cycle: Rights and Ethics in a Big Data World" (2017) UNICEF Office of Research – Innocenti Working Paper WP-2017- 06.

Bicker John et al, "Submission to the Office of the Privacy Commissioner of Canada in Response to the Notice of Consultation and Call for Essays — Online Reputation" (2016) Report for the Office of the Privacy Commissioner, online: <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/submissions-received-for-the-consultation-on-online-reputation/or/sub_or_10/>.

Blum-Ross Alicia & Livingstone Sonia, "'Sharenting", parenting blogging, and the boundaries of the digital self" (2017 April 17) 15:2 Intl J of Media and Culture 110 at 111.

Boyd Danah, “Why Youth (Heart) Social Networks Sites: The Role of Networked Publics in Teenage Social Life” (2007) Youth, Identity, and Digital Media, David Buckingham, ed., The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning, The MIT Press.

Gajda Amy, “Privacy, Press and the Right to be Forgotten I the United States” (2018) 93:201 Washington L Review 201.

Holloway Donell, “Surveillance capitalism and children’s data: The Internet of toys and things for children” (2019) 170:1 Media International Australia 27.

Lee James, “SB 568: Does California’s Online Eraser Button Protect the Privacy of Minors?” 48:1173 University of California, Daivs 1173 at 1203.

Lupton Deborah, “The use and value of digital media for information about pregnancy and early motherhood: a focus group study” 16:171 BMC Pregnancy and Childbirth.

Lupton Deborah & Pederson Sarah, “An Australian survey of women's use of pregnancy and parenting apps” 29:4 Women & Birth 368.

Lupton Deborah, Pederson Sarah & Thomas M Garreth, “Parenting and Digital Media: From the Early Web to Contemporary Digital Society” 10:8 Sociology Compass 730.

Lupton Deborah & Williamson Ben, “The datafied child: The dataveillance of children and implications for their rights” (2017) 19:5 New Media & Society 780.

Nyst Carly, “Privacy, Protection of Personal Information and Reputation” (2017) UNICEF Discussion Paper Series: Children’s Rights and Business in a Digital World.

Ouvrein Gaëlle & Verswijvelpage Karen, “Sharenting: Parental adoration of public humiliation? A focus group study on adolescents’ experiences with sharenting against the background of their own impression management” (2019) 99 Children and Youth Services Review 319.

Reiman H. Jeffrey, “Privacy, Intimacy, and Personhood” (1976) 6:1 Philosophy & Public Affairs 26.

Steinberg B. Stacey, “Sharenting: Children’s Privacy in the Age of Social Media” (2017) 66 Emory LJ 839.

Secondary Materials: Books

Barendt Eric, *Privacy* (London: Routledge, 2001).

Lievens Eva, *Protecting Children in the Digital Era: the Use of Alternative Regulatory Instrument* (Leiden, Boston: Marthinus Nijhoff Publishers, 2010).

Leaver Tama, “Born Digital? Presence, Privacy and Intimate Surveillance” in Hartley, John & W. Qu, ed, *Re-Orientation: Translingual Transcultural Transmedia.* (Shanghai: Fudan University Press, 2015) 149 at 151.

Secondary Materials: Online Sources

Battersby Lucy, “Millions of social media photos found on child exploitation sharing sites”, *The Sydney Morning Herald* (30 September 2015), online: <https://www.smh.com.au/national/millions-of-social-media-photos-found-on-child-exploitation-sharing-sites-20150929-gjxe55.html>.

BabyConnect, online: <https://www.babyconnect.com>.

Brisson-Boivin Kara, “The Digital Well-Being of Canadian Families” (2018) MediaSmarts, online (pdf): <https://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/digital-canadian-families.pdf>.

Children’s Commission, “Who Knows what about me?” (November 2018), online: <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/11/cco-who-knows-what-about-me.pdf> at 14.

C.S. Mott Children’s Hospital, “National Poll on Children’s Health” (16 March 2015), online: *Parents on Social Media Dislikes of Sharenting* <https://mottpoll.org/sites/default/files/documents/031615_sharenting_0.pdf>.

Feedspot, “100 Family Youtube Channels By Family Youtubers” (last updated May 10, 2020), online: <https://blog.feedspot.com/family_youtube_channels/>.

Harwell Drew, “Is your pregnancy app sharing your intimate data with your boss?” *The Washington Post* (10 April 2019), online: <https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an- app-may-be-more-public-than-you-think/>.

HDCYT, “Charlie bit my finger – again !” (22 May 2007), online (video): *YouTube* <https://www.youtube.com/watch?v=_OBlgSz8sSM>.

Law Offices of Salar Atrizadeh, “Privacy Rights for California Minors” (18 December 2017), online (blog): <https://www.internetlawyer-blog.com/privacy-rights-california-minors/>.

Lichtenstein Frederike et al, “Growing up on YouTube – How family vloggers are establishing their children’s digital footprints for them” (23 October 2007), online: *New Media & Digital Culture M.A, University of Amsterdam* < https://mastersofmedia.hum.uva.nl/blog/2017/10/23/growing-up-on-youtube-how-family-vloggers-are-establishing-their-childrens-digital-footprints-for-them/>.

Masters David, “Two British brothers have made internet history by clocking up 250 Million YouTube hits” (20 July 2010), online: *The Sun* <https://en.wikipedia.org/wiki/Charlie_Bit_My_Finger#cite_note-Masters-8>.

Nominet, “Share with Care” (2016), online: <https://media.nominet.uk/wp-content/uploads/2016/09/Nominet-Share-with-Care-2016-Infographic.pdf>.

Privacy Commissioner of Canada, “Guidelines for obtaining meaningful consent” (last modified 24 May 2018), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/>.

Privacy Commissioner of Canada, “Obtaining meaningful consent” (last modified 12 July 2019), online: <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/info_mc/>.

“Sharenting” (last modified 20 August 2013), online: *Collins Dictionary* <https://www.collinsdictionary.com/submission/11762/Sharenting>.

Steinberg Laurence, “Puberty, Cognitive transition, Emotional transition, Social transition”, online (blog): *Adolescence* <https://psychology.jrank.org/pages/14/Adolescence.html>.

Stacey Steinberg, “How Europe’s ‘right to be forgotten’ could protect kids’ online privacy in the U.S.” *The Washington Post* (11 July 2018), online: <https://www.washingtonpost.com/news/parenting/wp/2018/07/11/how-europes-right-to-be-forgotten-could-protect-kids-online-privacy-in-the-u-s/>.

StoryTrender, “Charlie Bit My Finger 10 Year Anniversary” (21 May 2017), online (video): *YouTube* <https://www.youtube.com/watch?v=bOuu_3-gAn0>.

The Report of the Nova Scotia Task Force on Bullying and Cyberbullying, “Respectful and Responsible Relationships: There’s No App for That” (29 February 2012), online: <http://antibullying.novascotia.ca/sites/default/files/Respectful%20and%20Responsible%20Relationships%2C%20There%27s%20no%20App%20for%20That%20-%20Report%20of%20the%20NS%20Task%20Force%20on%20Bullying%20and%20Cy berbullying.pdf>.