Sharenting Is Here to Stay, So Now What?

*Anonymous**

CONTENTS

INTRODUCTION: WHAT IS SHARENTING AND WHY IT MATTERS

Many parents[1] monitor what their children view on the internet because they are fearful of who or what they may encounter online.[2] There

* The author of this Note has chosen to stay anonymous.

1. This Note uses the word "parent" to refer to all primary caregivers of children, whether biological or not.

2. *See, e.g.*, Naline Lai & Pamela Harrington, *Screen Time: Know Your Child's Limits,* CHILD.'S HOSP. OF PHILA. (Oct. 15, 2019), https://www.chop.edu/news/health-tip/screen-time-know-your-child-s-limits [https://perma.cc/3MFR-N2XB]; Jeff Glor, *Making a Case for Spying on Kids' Online Activities*, CBS NEWS (Aug. 18, 2013), https://www.cbsnews.com/news/making-a-case-for-spying-on-kids-online-activities/ [https://perma.cc/MGU8-H3ZW].

are many tools that allow parents to do this.[3] The law also reinforces the parents' right to control their children's online presence.[4] However, while parents and lawmakers are focused on protecting children from third parties on the internet, little has been done to protect children's privacy interests against the effects of "sharenting."

A "sharent" is a parent who "frequently use[s] social media to share photos or other details and information about [their] child."[5] Sharenting[6] often starts before the baby is born, when proud parents-to-be post a sonogram photo on social media,[7] and continues from there. "Child" is defined as any person under the age of eighteen.[8] This definition encompasses a wide range of exploitative acts, from physical injury to sexual abuse.[9] A staggering 92% of two-year-old children in the United States have an online presence.[10] Many parents understandably want to share milestones, such as their baby's first steps, birthdays, and graduations.[11] Social media allows parents to instantly share these special moments with family and friends in a way that never used to be possible.[12] On Facebook alone, between 66% and 98% of parents post pictures of their children.[13] However, there is a blurry line between sharing and oversharing.

Sharenting has real-world consequences. A social media post of a child's birthday celebration can provide valuable information to online predators—the child's age, birthdate, location, and photographs. Parents have lost custody of their children due to sharenting.[14] Now, more than

---

3. Erin Dower, *10 Apps for Parents to Monitor Kids' Mobile Use*, FAM. EDUC., https://www.familyeducation.com/10-apps-for-parents-to-monitor-kids-mobile-use [https://perma.cc/DM8F-QZRK].

4. *See* 15 U.S.C. § 6501–06.

5. Sharent, DICTIONARY.COM, https://www.dictionary.com/browse/sharent?s=t [https://perma.cc/CWU8-23T3].

6. Sharent can be used as both a noun and a verb. *Id.*

7. Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 EMORY L. J. 839, 849 (2017).

8. 15 U.S.C. §6501(2).

9. *Id.*

10. Steinberg, *supra* note 7, at 848.

11. *See* Samantha Olson, *Consequences of "Sharenting": Parent Online Social Media Posts May Create Digital Identity for Child*, MED. DAILY (Mar. 18, 2015), https://www.medicaldaily.com/consequences-sharenting-parent-online-social-media-posts-may-create-digital-identity-326216 [https://perma.cc/GK2Q-RA62].

12. *Id.*

13. Tehila Minkus, Kelvin Lui & Keith W. Ross, *Children Seen but Not Heard: When Parents Compromise Children's Online Privacy*, 2015 INT'L WORLD WIDE WEB CONF. STEERING COMM. 776, 776 , http://cse.poly.edu/~tehila/pubs/WWW2015children.pdf [https://perma.cc/FL7B-BMR3].

14. Alex Hern*, FamilyOFive: YouTube Bans "Pranksters" After Child Abuse Conviction*, GUARDIAN (July 19, 2018), https://www.theguardian.com/technology/2018/jul/19/youtube-bans-familyofive-pranksters-michael-heather-martin-child-abuse-conviction [https://perma.cc/E4P7-ERZV].

ever, data brokers are profiting from the oversharing of children's information on the internet.[15] These are just a few examples. Creating a workable solution to adequately address the consequences of sharenting is a daunting task;[16] the competing interests between parents' and children's rights make solving the issue especially difficult.[17]

Part I of this Note provides a broad overview of sharenting and its implications. Part II describes the current state of the law and why sharenting remains a difficult issue to address. Part III discusses four legal frameworks posed by legal scholars to combat sharenting: anti-bullying, privacy, erasure, and child labor laws—and, ultimately, why each fails to offer an airtight solution. Part IV offers an alternative solution: the regulation of data brokers and outlawing advertisement-based social media platforms to protect children's online privacy.

I. THE DANGERS OF SHARENTING

A. The Physical and Emotional Consequences

Parents are increasingly using social media as a platform to shame their children as a form of punishment.[18] A common trend is for parents to give their kids embarrassing haircuts and then share pictures or videos online.[19] Other trends include parents live-streaming themselves destroying their kids' toys, filming their kids holding humiliating signs, and forcing their kids to reveal embarrassing secrets to the camera.[20] One dad made his child run a mile to school in the rain as he drove behind, filming it and posting it for the world to see.[21] These videos have sparked debate over public humiliation as a form of punishment.[22] This type of shaming "can have long-term effects that carry over into adulthood, impacting the individual's identity, self-esteem, and relationships with others."[23]

Parents pranking children and posting it on social media is another growing trend. In recent years, late-night television host Jimmy Kimmel

---

15. LEAH A. PLUNKETT, SHARENTHOOD: WHY WE SHOULD THINK BEFORE WE TALK ABOUT OUR KIDS ONLINE 33 (2019).

16. PLUNKETT, *supra* note 15, at 55–59; *see* Steinberg, *supra* note 7, at 883.

17. PLUNKETT, *supra* note 15, at 79; Steinberg, *supra* note 7, at 861.

18. Steinberg, *supra* note 7, at 848; Susan A. Knight, *Technology Trends: Social Media Shaming—Parenting Strategy Failure*, 15 SOC. WORK TODAY, Nov.–Dec. 2015, at 8, 8 [https://perma.cc/7PJG-ZYW8].

19. Knight, *supra* note 18.

20. Daily Mail TV, *More Parents Posting 'Child-Shaming' Videos on Social Media*, YOUTUBE (May 3, 2018), https://www.youtube.com/watch?v=Bj_jJuOHBVw [https://perma.cc/F87B-W6WA].

21. *Id.*

22. *Id.*

23. Knight, *supra* note 18.

has instigated a Halloween prank that has become an internet sensation.[24] Each year, he has parents tell their kids they ate all their Halloween candy and capture the inevitable meltdowns on camera.[25] In a recent Twitter trend, parents threw pieces of cheese at their toddlers' foreheads and filmed their stunned reactions.[26] While parents intend for these pranks to be playful, they should stop to consider the emotional consequences these acts can have on a developing child.[27]

Some pranks cross the line into abuse. In 2018, YouTube vloggers Michael and Heather Martin lost custody of two of their children after being convicted of child neglect for posting videos of them "pranking" their kids by screaming profanities at them and breaking their toys.[28] In one video, Michael Martin prompts his son to slap his daughter in the face.[29] Disturbingly, they had over 75,000 subscribers to their YouTube channel and had over 176 million views on their videos.[30]

In severe cases,[31] social media gives a platform to parents who are willing to exploit their children for a "like" or a "view." Nevertheless, even the most well-intentioned parents may inadvertently put their kids in danger by sharing their information on the internet. For example, a seemingly innocuous "Happy Birthday!" post about one's baby could allow an online predator to gather important information about the child, including a photo of the child's face, birthdate, name, and even location.[32] This is dangerous because child pornography is one of the most prolific online businesses, and photos of children posted to Facebook and Instagram can make their way to nefarious sites without the parents ever

---

24. Maya McDowell, *How to Get Featured in Jimmy Kimmel's Annual Halloween Candy Prank*, DELISH (Oct. 31, 2018), https://www.delish.com/food-news/a24481373/how-to-get-featured-jimmy-kimmels-halloween-candy-prank/ [https://perma.cc/95W3-K3AR].

25. *Id.*; Jimmy Kimmel Live, *YouTube Challenge–I Told My Kids I Ate All Their Halloween Candy*, YOUTUBE (Nov. 2, 2011), https://www.youtube.com/watch?v=_YQpbzQ6gzs [https://perma.cc/ZCC2-NG4Y].

26. Christian Gollayan, *Viral 'Cheese Challenge' Has Adults Throwing Cheese at Babies*, FOX NEWS (Mar. 2, 2019), https://www.foxnews.com/lifestyle/viral-cheese-challenge-adults-babies-twitter-throw [https://perma.cc/PZN2-L8EG].

27. Children who are repeatedly the targets of pranks by their parents may experience anxiety, depression, bullying, and aggression. Tracy S. Bennett, *How Online Parent Pranking May Be Child Abuse*, GET KIDS INTERNET SAFE, https://getkidsinternetsafe.com/childabuse [https://perma.cc/JF2J-SJQD].

28. Sam Levin, *Couple Who Screamed at Their Kids in YouTube 'Prank' Sentenced to Probation*, GUARDIAN (Sept. 12, 2017), https://www.theguardian.com/us-news/2017/sep/12/youtube-parents-children-heather-mike-martin [https://perma.cc/5ZX5-29ML].

29. Hern*, supra* note 14.

30. Levin, *supra* note 28.

31. *See, e.g.*, *id.*

32. Minkus, Lui & Ross, *supra* note 13, at 776–80.

knowing.[33] Predators can turn non-salacious photos, like a baby at bath time or even just a photo of a child's face, into pornographic content.[34] A predator who is savvy enough to match a parent's Facebook page to his voter registration could gather even more information, such as an exact address.[35]

Additionally, the risk does not necessarily decrease when the parent attempts to increase their privacy protections.[36] For example, changing their social media privacy settings to be viewable to "friends-only" is insufficient because most crimes against children are at the hands of someone the child knows.[37] Therefore, a parent with a Facebook account set on private but who posts information depicting their child's location may be putting their child in as much danger as if the post were viewable to the public.

B. Breach of Privacy Consequences

Crimes that threaten a child's physical and emotional safety are not the only risk of sharenting. Parents also need to consider their children's privacy interests and the long-term effects of not protecting those interests. It is estimated that by 2030, nearly two-thirds of identity theft of today's children will result from sharenting.[38] Additionally, by archiving every moment of a child's maturation in a public forum, parents create the child's social identity before the child can decide who they are and what sort of online presence they want to have. Parents may post information that a child finds too personal once they are older, and they will have little to no control over who sees it at that point;[39] accordingly, "[a] conflict of interests exists as children might one day resent the disclosures made years earlier by their parents."[40] This includes parents who share information about their kids on social media to connect with loved ones, as well as a growing sub-group of parents who share intimate details of their children's

---

33. *See, e.g.*, Sue Scheff, *Are You a Parent or a "Sharent"?,* CONNECTSAFELY (June 24, 2015), https://www.connectsafely.org/are-you-a-parent-or-a-sharent/ [https://perma.cc/N2P9-85G8].

34. *Id.* ("According to National Center for Missing and Exploited Children, as of June 2014, the CyberTipline has received more than 2.5 million reports of suspected child sexual exploitation since it was launched in 1998, and ICAC Task Forces noted a more than 1,000% increase in complaints of child sex trafficking.").

35. Minkus, Lui, & Ross, *supra* note 13, at 776–80.

36. *Id.* at 777.

37. In 1997, the FBI published data that show family members or acquaintances perpetrated 76% of kidnappings and 90% of violent crimes against children. *Id.*

38. Hua Hsu, *Instagram, Facebook, and the Perils of 'Sharenting,"* NEW YORKER (Sept. 11, 2019), https://www.newyorker.com/culture/cultural-comment/instagram-facebook-and-the-perils-of-sharenting [https://perma.cc/ARK7-ESWU].

39. Olson, *supra* note 11.

40. Steinberg, *supra* note 7, at 839.

lives for financial gain.[41] This practice of "commercial sharenting"[42] can be especially threatening to a child's privacy interests because it curates a public identity of the child that may or may not be how the child wants to be known in adulthood.

The children who are the subjects of sharenting today will soon be young adults applying to colleges, graduate schools, and jobs, running for political office, and looking for romantic partners. They are the first generation who has had their entire existence documented online without their consent.[43] Before taking their first step, "their digital data [have] already travel[ed] to 'thousands, likely tens of thousands, of human and machine users.'"[44] And once an image or video is online, it is nearly impossible to remove it.[45] As a result, it is easy to imagine a not-so-distant future in which a child's online dossier predetermines the opportunities he will have—or not have—later in life.[46]

Leah Plunkett, a law professor at University of New Hampshire and author of *Sharenthood: Why We Should Think Before We Talk About Our Kids Online*, describes a frightening yet believable scenario in which companies (and perhaps the government) will begin to predict who a child will be as an adult, based on data points assigned to their tastes or allegiances, beginning at conception.[47] Plunkett foresees a system in which children's development is tracked online and translates into a "personal capital score."[48] This could be comparable to China's "social credit system."[49]

In our increasingly digital world, we are constantly giving our information to data brokers who aggregate and analyze our digital data, then sell it to third parties for profit.[50] Data brokers are loosely regulated, and children's data is extremely valuable to them.[51] Currently, key markets for children's data include "credit, insurance, education, and employment," but this is likely to expand.[52] By using the information

41. PLUNKETT, *supra* note 15, at 55–59.

42. *Id.* at 55.

43. *See generally* Steinberg, *supra* note 7.

44. Hsu, *supra* note 38.

45. *See* Diana Brown, *Can You Really Delete Your Internet History?*, HOWSTUFFWORKS.COM (Oct. 3, 2017), https://computer.howstuffworks.com/can-you-delete-internet-history.htm [https://perma.cc/U5HV-6AZY].

46. *See* PLUNKETT, *supra* note 17 at 101; Hsu, *supra* note 38.

47. PLUNKETT, *supra* note 15, at 101.

48. *Id.*

49. Nicole Kobie, *The Complicated Truth About China's Social Credit System*, WIRED (June 7, 2019), https://www.wired.co.uk/article/china-social-credit-system-explained [https://perma.cc/AE2L-BVSE].

50. PLUNKETT, *supra* note 15, at 32–34.

51. *See id.* at 33.

52. *Id.*

parents share online, data brokers can make profiles of children that can be continually updated throughout their lives.[53] For example, colleges already look at applicants' social media profiles.[54] When combined with test scores and demographics obtained by data brokers, colleges could use predictive analytics to determine the probability of whether a student will be successful by their standards.[55]

Additionally, the consumer credit industry is already looking for ways to assess credit scores based on people's social media presence.[56] It is possible that what parents say about their children online now could become part of the assessment of their qualification for a credit card or a loan in the future.[57] In short, "the gatekeepers to services and opportunities that are likely to matter most to young people's futures are using digital data trails to decide whether gates open or stay barred."[58] Therefore, a child's digital presence is not merely a matter of data brokers gathering and selling data; data brokers' true interest lies in shaping the trajectory of kids' lives for their clients' financial gain.[59]

II. THE CURRENT STATE OF THE LAW

Generally, the law gives deference to parents in determining how to raise and protect their children.[60] Yet, when parents fail to protect their children from physical exploitation or abuse, the government steps in to ensure their safety. This interference is because our society recognizes that children are vulnerable and unable to adequately protect themselves from harm, especially at the hands of adults.

Physical and psychological abuse or neglect are extremely detrimental to a child's health and development.[61] Accordingly, all states have enacted laws against child abuse and neglect.[62] For example, in Washington, abuse or neglect is defined as "sexual abuse, sexual exploitation, or injury of a child by any person under circumstances which

53. Minkus, Lui, & Ross, *supra* note 13, at 777.

54. PLUNKETT, *supra* note 15, at 35.

55. *See id.*

56. *Id.*

57. *See id.*

58. *Id.*

59. *Id.* at 29.

60. Parents enjoy the constitutional right to raise their children the way they sit fit. *See* Meyer v. Nebraska, 262 U.S. 390, 399 (1923) (recognizing that a parent's right to control their child's upbringing and education is protected by the Due Process Clause of the Fourteenth Amendment).

61. CHILDS.' BUREAU, U.S. DEP'T OF HEALTH & HUM. SERV'S., LONG-TERM CONSEQUENCES OF CHILD ABUSE AND NEGLECT (2019), https://www.childwelfare.gov/pubPDFs/long_term_consequences.pdf [https://perma.cc/Z4RG-7BSZ].

62. *See, e.g.*, *State Laws on Child Abuse and Neglect*, U.S. DEP'T OF HEALTH & HUM. SERV'S., https://www.childwelfare.gov/topics/systemwide/laws-policies/can/ [https://perma.cc/S76B-PWA8].

cause harm to the child's health, welfare, or safety . . . or the negligent treatment or maltreatment of a child by a person responsible for or providing care to the child."[63]

Washington law defines "negligent treatment or maltreatment" as "an act or a failure to act, or the cumulative effects of a pattern of conduct, behavior, or inaction, that evidences a serious disregard of consequences of such magnitude as to constitute a clear and present danger to a child's health, welfare, or safety . . . ."[64] While the conduct of oversharing parents, like the Martins,[65] clearly falls within the definition of child abuse, most sharenting is not this egregious. When it does not rise to the level of child abuse, the harm caused by sharenting is a gray area under the law and parents hold the rights to their children's privacy. Thus far, the legislature and courts have failed to recognize and protect children from the harm that occurs through the exploitative nature of non-abusive sharenting.

One reason for the lack of legislation is this is the first generation of children to be showcased on the internet to such an extreme level, and it is occurring in conjunction with the ever-expanding ability of data brokers to collect and use data.[66] Therefore, we have yet to see the full scale of harm that sharenting will cause, and the law naturally takes time to react to new threats. Another reason for the lack of legislation is parents are the gatekeepers of their children's personal information under the law.[67] Thus, the law presumes parents will keep their children's information safe.

Without intervening legislation, parents are free to share their children's information as they wish. Unfortunately, this fails to account for the fact that in today's social-media-obsessed society, parents are often exploiting their children's privacy on the internet. Children do not have the capacity to truly consent to what their parents post about them online, nor do they understand the long-term consequences of their online presence. Therefore, we must protect children through legislation from exploitative sharenting until they are old enough to protect themselves, just as we protect children from other forms of exploitation.[68]

While it is difficult to draw the line between a parent's freedom to share and a child's right to privacy, the legislature must establish laws to

63. WASH. REV. CODE § 26.44.020(1) (2018).

64. *Id.* at § 18.

65. *See* Levin, *supra* at note 28.

66. *See supra* Section I.B.

67. *See* 15 U.S.C. § 6501–06.

68. Throughout the rest of this Note, when I refer to sharenting I do not mean the type of sharenting that rises to the level of child abuse, for which there is a remedy in criminal law. *See generally* CHILDS.' BUREAU, U.S. DEP'T OF HEALTH & HUM. SERV'S., *supra* note 61. Instead, I am referring to the majority of the sharenting that occurs today—well-intentioned parents who share every milestone and mundane moment of their children's lives online, not recognizing or ignoring the inherent risks associated with such behavior.

ensure that children own the right to shape their reputation and sense of self as they mature.

III. AN OVERVIEW OF POSSIBLE LEGAL FRAMEWORKS AND THEIR PITFALLS

Combined, Plunkett's and University of Florida law professor Stacey Steinberg's research covers a wide gambit of possible legal frameworks to curb the negative effects of sharenting. Unfortunately, as they acknowledge, none offer a perfect solution. This Part will discuss several possible frameworks and their pitfalls, to provide a clear understanding of the work that has been done in this area to date and a starting point for future discussion around this important topic.

A. Anti-Bullying Laws

Many states have passed new legislation in recent years to address bullying between children and teens.[69] Cyberbullying has become an increasing threat to adolescents, as more and more of their social interactions take place over the internet.[70] Plunkett suggests that some instances of sharenting should be considered cyberbullying, such as those within the popular genre of parental prank videos,[71] and could be dealt with by state anti-bullying laws.[72]

For example, New Hampshire defines bullying as "a single significant incident or a pattern of incidents involving a written, verbal, or electronic communication, or a physical act or gesture, or any combination thereof, directed at another pupil which . . . causes emotional distress to a pupil."[73] Under this law, bullying includes "actions motivated by an imbalance of power based on a pupil's actual or perceived personal characteristics . . . ."[74] As Plunkett points out, the word "pupil" makes clear that this law applies only in the school context;[75] however, Plunkett suggests that one could replace the word "pupil" with the word "minor," broadening its scope such that it applies to any incident that causes a person under the age of eighteen emotional distress, including when motivated by the imbalance of power associated with difference in age—

69. *See, e.g.*, PLUNKETT, *supra* note 15, at 65.
70. *Id.*
71. *See supra* Section I.A.
72. PLUNKETT, *supra* note 15, at 65.
73. N.H. REV. STAT. Ann § 193-F:3(I.)(a) (2010).
74. *Id.* at (I.)(b).
75. PLUNKETT, *supra* note 15, at 66.

like a parent and child.[76] Written this way, the law could cover incidents such as the Halloween candy prank.[77]

However in practice, a law like this risks being unconstitutionally overbroad[78] because "it could prohibit positive parenting conduct that keeps your child safe, like making your thirteen-year-old cry when you tell him he can't drive your car because he's underage."[79] Additionally, this type of law runs the risk of intruding too far into the constitutional protection that parents enjoy to parent and raise a family in the way that they see fit.[80] Thus, this seemingly simple solution to change one word in the anti-bullying laws fails to adequately address the issue of sharenting.

B. Privacy Laws

Consumer privacy, as it relates to the collection, use, and disbursement of personal identification information online, takes a consent-based approach.[81] Under the federal Children's Online Privacy Protection Act (COPPA),[82] parents must give consent for websites to gather information about children under age thirteen.[83] If violated, the parent or state can bring suit under the Federal Trade Commission's protection against unfair or deceptive practices.[84] This burden of initiating the lawsuit puts the onus of data protection on the individual rather than on the company who wants to use the data. It assumes that people will not only read, but understand, what they are consenting to when they agree to the privacy policies and terms of use encountered on nearly all web-based services.[85] It also assumes that companies are transparent about their privacy policies while in reality most are not.[86] Thus, this is an unrealistic approach to protecting children's data because the average parent-

76. *Id.*

77. *Id.*

78. "A law is constitutionally overbroad if it regulates substantially more speech than the Constitution allows to be regulated and a person to whom the law constitutionally can be applied can argue that it would be unconstitutional as applied to others." THE LAW DICTIONARY, https://thelawdictionary.org/constitutional-law/ [https://perma.cc/ZZF3-2DF7].

79. PLUNKETT, *supra* note 15 at 66.

80. *See id.*; *see also* Meyer v. Nebraska, 262 U.S. 390, 399 (1923) (recognizing that a parent's right to control his child's upbringing and education is protected by the Due Process Clause of the Fourteenth Amendment).

81. *See* PLUNKETT, *supra* note 15 at 80.

82. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–06 (2012).

83. Steinberg, *supra* note 7, at 870.

84. *Id.* at 870–71.

85. PLUNKETT, *supra* note 15, at 80.

86. *See id.* ("We are expected to find, read, and understand the relevant privacy policies . . . that define what a third party wants to do with our children's digital data." However, "reading and understanding all the fine print [is] difficult if not impossible.").

consumer will not wade through confusing, and often hard-to-find, privacy policies, let alone understand if there is a breach.

Moreover, companies like Facebook and Google have many incentives to share the data they collect.[87] Google and Facebook are modern-day data brokers.[88] They make their money by selling individual's online data and have been known to find ways around their privacy obligations when it suits them.[89] While it is unrealistic to expect parents to adequately protect their children's data through the current consent-based model, it is also unrealistic to think that social media platforms and other websites will safeguard children's data shared by parents and keep it for themselves due to the profitability of human data. Thus, privacy laws in their current form do not offer a comprehensive solution to protecting children's online identities.

However, the federal Health Insurance Portability and Accountability Act (HIPAA) and Family Educational Rights and Privacy Act (FERPA) currently offer the most comprehensive framework for protecting children's data in the United States.[90] They prohibit third-parties from releasing children's personal information, such as the child's name, address, age, grades, health and behavior records, without parental consent.[91] And, once the child turns eighteen, he must give consent before his information can be released.[92] However, these laws only safeguard children's data from being released by third-parties, not parents.[93] By their very design, they give parents complete control over the release of their children's records.[94]

While these laws recognize that children have a legitimate interest in keeping their private information secure, "in the context of parental sharing, the third-party actor is the parent, and therefore a conflict exists between the actor and the party authorized to give consent."[95] Thus, these laws are insufficient to address the dangers of sharenting because the

87. Chris Hoofnagle, *Facebook and Google Are the New Data Brokers,* DIGITAL LIFE INITIATIVE (Dec. 18, 2018), https://www.dli.tech.cornell.edu/post/facebook-and-google-are-the-new-data-brokers [https://perma.cc/FSS5-8ECP].

88. *Id.* Traditional data brokers sell consumer information for profit. *Id.* Modern-day data brokers, such as Facebook and Google, trade consumer information to developers in exchange for new and innovative ways to increase the time users spend on their platforms. *See id.*

89. *Id.* For example, in exchange for Blackberry integrating Facebook into its phones, Facebook made Blackberry a "service provider" with privileged access to Facebook users' data, overriding users' privacy settings. *Id.*

90. PLUNKETT, *supra* note 15, at 81.

91. Steinberg, *supra* note 7, at 872–73.

92. *Id.*

93. *Id.*

94. *Id.*

95. *Id.* at 873.

parent can share the same information protected by these laws on social media.

Theoretically, the state could act as a check to parental oversharing, stepping in to enjoin parents from posting any potentially harmful details. However, "a censorship argument of this type would likely fail as an unreasonable restraint against speech under the prior restraints doctrine,"[96] unless the posts rise to the level of neglect or abuse.[97] Thus, while HIPAA and FERPA serve an important role in protecting children's data, they do not serve as a workable framework for addressing sharenting.

C. Eraser Laws

In 2015, California was the first state to pass an "Online Eraser" law, which allows children under the age of eighteen who live in California to remove or request to remove content or information that they post on an internet operator's website.[98] This law is similar to COPPA, except it broadens the protected age range and applies only to kids living in California.[99] In its current form, the Online Eraser law only seeks to protect children from oversharing about themselves; it does not protect children from the oversharing parent.[100] Theoretically, the eraser law framework could serve as a guide to create laws that protect children's digital privacy against the oversharing parent. The same way that websites must allow children in California to "scrub away their online indiscretions," children could also be allowed to delete information others share about them.[101] However, as critics of the law point out, there are pitfalls of the Online Eraser law that render it insufficient to protect children's online privacy, even if it were expanded to include information shared by others.

Critics of the California law suggest that while trying to protect children, this law may actually put children more at risk because websites will have to gather more information about their users in order to comply

---

96. *Id.*

> The concept of prior restraint, roughly speaking, deals with official restrictions imposed upon speech or other forms of expression in advance of actual publication. Prior restraint is thus distinguished from subsequent punishment, which is a penalty imposed after the communication has been made as a punishment for having made it.

Thomas I. Emerson, *The Doctrine of Prior Restraint*, 20 L.& CONTEMP. PROBS. 648, 648 (1955).

97. Steinberg, *supra* note 7, at 873.

98. CAL. BUS. & PROF. CODE § 22580 (West 2019); Rahul Kapoor, W. Reece Hirsch & Shokoh H. Yaghoubi, *Get to Know California's 'Online Eraser' Law*, NAT'L L. REV. (July 12, 2016), https://www.natlawreview.com/article/get-to-know-california-s-online-eraser-law [https://perma.cc/XSK3-CPUL].

99. Kapoor, Hirsch & Shokoh, *supra* note 100.

100. Somini Sengupta, *Sharing, with a Safety Net*, N.Y. TIMES (Sept. 19, 2013), https://www.nytimes.com/2013/09/20/technology/bill-provides-reset-button-for-youngsters-online-posts.html [https://perma.cc/3BGL-QNPZ].

101. *Id.*

with the law (such as whether the user is eighteen years old and lives in California).[102] Another unintended consequence may be that if other states follow suit, it will create an extremely complicated scenario for online companies trying to adhere to varying state laws and gather appropriate information about children from each state.[103] Children would be better protected if a uniform set of national rules regulated the internet rather than individual state rules.

One of the biggest pitfalls of the Online Eraser law is that, as its name suggests, it tries to remedy the damage retroactively. Sharenting should be regulated preemptively, rather than reactively, because once an image or piece of data is on the internet, it remains there to be rediscovered.[104] The California law does not require that companies remove the deleted material from their servers, so the material is not truly "deleted"; rather, it is stored out of one's direct sight.[105] Therefore, Online Eraser laws in this form are a good start and certainly serve a useful purpose, but they are insufficient to deal with the ever-increasing problem of sharenting.

D. Child Labor Laws

Some have suggested that child labor laws could protect children from the oversharing parent.[106] The theory is that parents who regularly post content of their children on social media platforms are receiving something of value in return—a "payment" of sorts.[107] For some parents, social media gives them a sense of community because it is a place to swap stories and commiserate about parenthood.[108] For others, it is a business because they receive monetary payments in exchange for their posts.[109] Nevertheless, all sharents have one thing in common: they all receive a service in return for their posts. Because social media runs on an advertisement-based business model, every person who uses these platforms trades his personal data for free access to the site.[110] Thus, in almost any scenario, parents who share their children's data on social media are receiving a service from sharing that data. In this sense, children

102. *Id.*
103. *Id.*
104. *See* Brown, *supra* note 45.
105. Sengupta, *supra* note 102.
106. *E.g.*, PLUNKETT, *supra* note 15, at 91.
107. *See id.* at 90.
108. *Id.* at 57.
109. *Id.* at 45 ("Some parents take this practice [sharenting] to a whole new level by monetizing kids' stories in the commercial sphere."). In this Note, I borrow the term "commercial sharenting" from Plunkett. *Id.* at 55.
110. *See id.* at 89.

are "employed" by their parents who profit from selling their children's personal data.[111]

Kids who constantly serve as fodder for their parents' social media accounts are deserving of the same protections as child actors. Often, parents who post videos of their kids online, especially those who do it for financial gain, are curating the experience as if on a movie set; they tell the kid what to say, how to say it, and how to behave so that they will receive the most views.[112] In the digital world, views translate into currency.[113]

The law protects child actors in various ways. For example, in some jurisdictions, the law protects child actors from parents who may squander the child's earnings.[114] In these jurisdictions, the law requires that a child actor's earnings are set aside in a trust to protect his financial interests from parents who may be inclined to exploit the child's talents for their own financial gain.[115] Perhaps commercial sharents should be required to set aside the money they earn—or a portion thereof—in a trust for their child, who is the real star of the show.

The law also recognizes that a child actor is an easy target for labor exploitation because he is unable to negotiate working conditions for himself. For that reason, some states have begun to tighten regulations related to child actors. In California, where most acting jobs are located, a child performer between the ages of fifteen and eighteen must have a permit to work and the employer must have a permit to employ the child.[116] Notably, the permit will not be issued if "the [working] environment is improper for the minor, the employment conditions are detrimental to the minor's health, or if the minor's education is hampered."[117] This law ensures that child performers' developmental needs are satisfied.

In the same way, the legislature could require parents who want to use their children to make social media content for financial gain to apply for a permit. The process of applying for and obtaining a permit would provide some oversight to ensure that the creation of social media content, and the potential stardom that follows, is not detrimental to the child's education, physical or mental health. Moreover, this would not interfere with parents' right to freely post content of their children unless it meets a

111. PLUNKETT, *supra* note 15, at 90.

112. *See id.* at 59.

113. *See id.* at 56.

114. *Id.* at 91.

115. *Id.*

116. DEP'T OF INDUS. RELS., DIV. OF LAB. STANDARDS ENF'T, CAL. CHILD LABOR LS. 36 (2013), https://www.dir.ca.gov/dlse/childlaborlawpamphlet.pdf.

117. *Id.*

certain financial or hourly threshold.[118] For example, a provision could state that if a parent earns more than $1,000 per year in money, goods, or services by posting content of his child, that child is considered a child actor under the law. Alternatively, the time spent creating content could formulate a provision: if a child appears in more than one hour of filmed content per week, that child is considered a child actor, subject to the same protections as child actors in movies and television shows.

However, both of the potential provisions outlined above would be hard to enforce. If the standard was based on income, regulatory authorities would have to rely on parents accurately self-reporting the income from their commercial sharenting endeavors. Moreover, most financial gain obtained from posting social media content comes from goods or sponsorships.[119] Therefore, putting an exact monetary value on it could be difficult for the parents to assess. Additionally, if the standard was based on hours, we would still have to rely on parents to accurately self-report. Because filming occurs in the privacy of the home, rather than a movie set, there are no set hours of production. A parent's camera might always be rolling. Alternatively, a parent may make a child do several takes to capture a moment that appears spontaneous, when it is actually curated. There is no easy way to account for all the time spent crafting these "perfect" moments.

Unfortunately, using child labor laws as a framework to control sharenting is flawed because it applies only to the sector of parents who share for commercial gain. It does not account for the harm caused by non-commercial sharenting.

At first glance, each of the four legal frameworks discussed above appears to provide a promising solution. However, a deeper analysis reveals the challenges of applying these existing laws to the context of sharenting. Thus, the challenge remains to provide a workable solution that does not impede parents' rights yet values and protects children's autonomy and privacy interests.

IV. A PATH FORWARD: REGULATING DATA BROKERS

Because of the rights afforded to parents as guardians of their children's privacy, it is difficult to see a legal path forward that inhibits parents from sharenting. Aside from extreme cases, like the Martin family, parents will, and should, continue to enjoy the right to share their children's information as they wish. To limit that choice would be to

118. A standard could be set that dictates how much a parent must be earning by posting content of his child online before it is necessary to obtain a permit.

119. PLUNKETT, *supra* note 15, at 55.

infringe upon a parent's constitutional rights.[120] While we, as a society, can hope to educate parents to make smart choices and understand the danger that sharenting poses, we cannot strip them of their rights. Instead, we must focus our legal efforts toward regulating the companies that make a profit from gathering and selling people's data. Companies such as Facebook, YouTube, and Google are modern-day data brokers with the ability to buy, trade, and sell our private information. Thus, society cannot hope to have meaningful control over sharenting unless companies are incentivized to protect children's privacy.

A. The Advertisement-Based Business Model

Platforms like Facebook and Google use an advertisement-based business model that allows users to access the service for free in exchange for viewing advertisements that are specifically geared toward them based on their personal data. This is good for the advertisers because they can reach a wider audience who is more likely to be interested in purchasing the product. It is also good for the platform hosting the advertisements because they can provide a free service to users, which attracts more people and gathers incomprehensible amounts of data to build their business. Some would even argue it is beneficial for the consumer because they get to use the platforms for free, so long as they are willing to put up with advertisements. And, if there are going to be advertisements, at least they are tailored to our particular interests. That rationale has allowed these companies to flourish in a nearly unregulated market. But whether there are actual benefits for the consumer and whether the consumers understand what they are trading for the ability to use these sites for free is up for debate. As one former Google developer said, "if you don't pay for the product, you are the product."[121] Thus, as long as this model continues in conjunction with sharenting, the data of our children will remain a profitable product for these companies.

B. The Subscription-Based Business Model

The advertisement-based model should be banned and replaced with a subscription-based system to better protect consumers, especially children. Many companies, such as Spotify, Pandora, and YouTube, already have subscription services as an option for those who prefer an advertisement-free experience. Other companies, like Netflix, require a subscription to use the service at all. As it currently stands, it is up to each

120. The First Amendment protects parents' rights to free speech, including on social media. *See* Steinberg, *supra* note 7, at 26. The Fourteenth Amendment protects parents' rights to raise children as they desire. *See supra* note 62 and accompanying text

121. THE SOCIAL DILEMMA (Netflix 2020).

individual company to decide which model it prefers to use: fully advertisement-based, fully subscription-based, or a mix of the two. Although a subscription-based system does inevitably cause a disparity between those who can afford to subscribe to the service and those who cannot, it is a more ethical approach than the current ad-based system that incentivizes the trade of human data for profit.

The national government should regulate data collection and dissemination to encourage continuity and enforceability.[122] The California Commercial Privacy Act (CCPA)[123] provides a useful model for Congress. "The CCPA gives individuals rights over their personal information, including the right to deletion, the right to know, and the right to opt out of the selling of personal information."[124] It defines personal information broadly as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[125] Using this broad definition of personal information, Congress should enact similar federal legislation. However, there is room to expand upon the broad definition of personal information; rather than providing the right to "opt out" of "selling personal information," it should instead ban businesses from "trading, selling or otherwise making available" any personal information of its consumers to advertisers or other third parties. This would force companies to decouple their business models from collecting and disseminating individual's personal data.

Parents are not going to stop sharing photos and information about their children online, and, for better or worse, social media is likely here to stay. As discussed throughout this Note, it is difficult to protect children from the consequences of sharenting by regulating the individual. Instead, by focusing on the data brokers—those who trade our information—we can reduce the value of children's data so that it no longer is a commodity worth trading. If Facebook earned a profit through paid subscriptions instead of advertisements, it would no longer have an incentive to trade personal data to advertisers. In such a world, sharenting would be far less detrimental to a child's autonomy. A child's data posted by his parents would not travel throughout the internet as it does now. A child's future opportunities would not be limited by a "personal credit score" that was created before he ever had a chance to influence it himself.

---

122. *See* discussion *supra* Section III(C).

123. CAL. CIV. CODE § 1798.140 (West 2020).

124. Sarah A. Sargent & Justin P. Webb, *California Consumer Privacy Act: A Practice Overview*, AM. BAR ASS'N (Apr. 12, 2020), https://www.americanbar.org/groups/litigation/committees/corporate-counsel/practice/2020/california-consumer-privacy-act-a-practice-overview [https://perma.cc/5FNY-5LEH].

125. CAL. CIV. CODE § 1798.140(v)(1) (West 2020).

CONCLUSION

If we continue allowing companies to make the rules, our children will continue to be the guinea pigs for data collection and implementation of new schemes to use that data. In a not-so-distant future, we may see that children today—those whose every move have been documented and shared online by parents—will be accepted or rejected, encouraged or discouraged, employed or unemployed, not because of the choices that they make, but because of their "social credit score," compiled by a lifetime of data that their parents gave up freely. We must ensure the safety and privacy of our kids' data until they are of age to determine what they want to share and what they want to keep private, and to do so in a way that respects parents' rights. The best course of action is to regulate the websites where parents post, respecting the parents' rights to share. Requiring a subscription-based business model will disincentivize the over-sharing of data that is rampant today, and by default, will protect children from the dangers of sharenting.