

FROM INNOCENT SHARING TO HARMFUL AND UNINTENDED
EXPOSURE: BALANCING PARENTAL RIGHTS AND
CHILDREN’S DIGITAL PRIVACY RIGHTS

*Perla Khattar**

Abstract

In the digital age, “sharenting”—the practice of parents sharing details of their children’s lives online—has become ubiquitous, blurring the lines between innocent sharing on social media and harmful exposure on the dark web. This Article delves into the complexities of balancing parental rights with children’s digital privacy rights, framed against the backdrop of a society increasingly reliant on social media for community and validation. By examining the legal and societal impacts of sharenting, it highlights the urgent need for legal frameworks that both respect parental autonomy and protect children’s online privacy. This Article proposes a multifaceted approach to address this challenge, advocating for comprehensive international legislation, enhanced social media platform policies, and increased awareness among parents of the potential long-term consequences of digital exposure. By integrating analysis of current laws, case studies, and international privacy standards, this Article contributes to the ongoing discourse on establishing a global privacy standard that safeguards children’s digital footprints, ensuring their autonomy and dignity online.

INTRODUCTION210

I. SHARENTING AND ITS DARK SIDE212

 A. *Sharenting: A Double-Edged Sword*212

 B. *Facts and Figures: The Hidden Realities of Sharenting*216

II. THE DISTURBING WORLD OF CHILD PORNOGRAPHY: AN EXAMINATION OF ITS FORMS AND TYPES218

 A. *Real Child Pornography*218

 B. *Virtual Child Pornography*220

 C. *Morphed Child Pornography*221

III. THE INCREASING GAP BETWEEN TECHNOLOGY AND THE LAW IN THE UNITED STATES: CHALLENGES FOR THE COURTS223

 A. *The Haunting Shadow of Sidis*223

 B. *The COPPA’s Inability to Protect Children*.....224

* Attorney at the Beirut Bar Association and Technology Ethics Fellow at IBM.

C.	<i>The Uphill Legal Battle</i>	226
D.	<i>The National Center for Missing and Exploited Children</i>	227
IV.	INTERNATIONAL HUMAN RIGHTS LAW, SHARENTING, AND DIGITAL PRIVACY	228
A.	<i>The Convention on the Rights of the Child</i>	228
B.	<i>The International Covenant on Civil and Political Rights</i>	229
C.	<i>The Council of Europe’s Convention on Cybercrime</i>	229
V.	BALANCING PARENTAL RIGHTS AND CHILDREN’S DIGITAL PRIVACY RIGHTS.....	231
	CONCLUSION.....	233

INTRODUCTION

In 2019, a mother by the name of Jacquelyn set up a TikTok account to document the childhood of her toddler W.E.¹ The then-unemployed Jacquelyn found that her popular daughter’s account “earns a lucrative income,” which led her to start posting more regularly.² However, as the account amassed more followers, reports suggested that W.E.’s content was being disseminated on the dark web and child pornography sites.³ A hashtag calling to save W.E. had been viewed over 173,000,000 times on TikTok,⁴ as Jacquelyn continued to post “sexualized content” of her daughter that did not violate any social media community guidelines or laws.⁵

While older generations are still figuring out how to manage their virtual reality, younger generations are losing their right to privacy and are accumulating massive digital footprints.⁶ Due to the W.E. controversy, parents are grappling with the dilemma of how to share their

1. Jacqueline Mey, *Dark Side of Social Media: Mum Forced to Defend Herself After Being Accused of ‘Exploiting’ Her Toddler On TikTok*, 7NEWS (Sept. 9, 2022), <https://7news.com.au/lifestyle/real-life/dark-side-of-social-media-mum-forced-to-defend-herself-after-being-accused-of-exploiting-her-toddler-on-tiktok-c-8287828> [<https://perma.cc/manage/create?folder=189838>].

2. *Id.*

3. *Id.*

4. #savewren, TIKTOK, <https://www.tiktok.com/tag/savewren> [<https://perma.cc/C3WV-T6GZ>].

5. Mey, *supra* note 1.

6. Kate Lindsay, *A Digital Footprint That Begins Before Birth*, SPOKESMAN-REV. (Apr. 10, 2023), <https://www.spokesman.com/stories/2023/apr/10/a-digital-footprint-that-begins-before-birth/> [<https://perma.cc/R8TC-ZNQF>].

children online, while protecting them from predators.⁷ An increasing number of parents are deciding to stop sharing their children online altogether, while others are opting to blur their little one's faces from videos and images.⁸

Millennials will be the last generation to have lived a life before the internet's proliferation,⁹ and Generation Z is "the first group of digital natives."¹⁰ This dystopian reality is largely because some parents have socially and monetarily capitalized on disclosing their children's information to millions of strangers online,¹¹ while others have resorted to social media to either find a virtual village¹² or to "make a digital record" for their children.¹³

This Article argues that the "most vulnerable and impressionable population in society," children, deserve to have their privacy protected online,¹⁴ and the most efficient way to protect children's privacy is through the establishment of international privacy protections. Part I explains the concept of sharenting and highlights alarming statistics. Part II examines the forms and types of child pornography. Part III brings attention to the increasing gap between technology, statutory, and case law in the United States. Part IV goes over international instruments that are often used to protect children's privacy. Finally, Part V evaluates proposals that seek to balance the parents' right to direct the upbringing of their child and the minors' right to digital privacy and proposes international privacy protection as a potential solution.

7. Mey, *supra* note 1.

8. Angela Brauer, *Why Parents Are Choosing Not to Post Their Kids Photos Online*, WGN-TV (Oct. 14, 2021), <https://wgntv.com/news/why-parents-are-choosing-not-to-post-their-kids-photos-online/> [<https://perma.cc/HN5R-E7YS>].

9. Edie Meade, *The Last Analogue Generation*, MEDIUM (Feb. 14, 2020), <https://medium.com/age-of-awareness/the-last-analogue-generation-f899cf40975d> [<https://perma.cc/7JCJ-8HRE>].

10. SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* 447 (2019).

11. See Emine Saner, *The "Sharent" Trap – Should You Ever Put Your Children on Social Media?*, THE GUARDIAN (May 24, 2018), <https://www.theguardian.com/lifeandstyle/2018/may/24/sharent-trap-should-parents-put-their-children-on-social-media-instagram> [<https://perma.cc/8NXH-DRG4>].

12. *Why New Parents Turn to a Virtual Village*, FACEBOOK (May 8, 2018), <https://www.facebook.com/business/news/insights/why-new-parents-turn-to-a-virtual-village> [<https://perma.cc/FKG3-RE6U>].

13. Mey, *supra* note 1.

14. Cole F. Watson, *Protecting Children in The Frontier of Surveillance Capitalism*, 27 RICH. J.L. & TECH., no. 2, 2021, at 5.

I. SHARENTING AND ITS DARK SIDE

Due to parents sharing sonogram images online, a lot of babies have an online presence while they are still in the womb.¹⁵ While most adults have a digital footprint that stretches back ten to fifteen years at most,¹⁶ a sizeable amount of children today have an online presence that starts when they are very young and continues to grow throughout their lives.¹⁷ However, the decision to share information online about one's child is linked to the parent's right to direct the upbringing of their child, one of the core values of American culture.¹⁸ And while it is generally true that parents have the best intentions for their children, their lack of awareness or understanding of certain issues may lead them to unintentionally overlook the consequences of sharenting.¹⁹

A. *Sharenting: A Double-Edged Sword*

Parents are regarded as the natural protectors of their children's analog and digital identities.²⁰ However, the intentional and often unintentional online disclosure of children's personally identifiable information (PII) can and does lead to harm in some cases.²¹ Ordinary people often become famous overnight on social media where nothing is off the table.²² Parents share content depicting either humorous, silly, or outrageous conduct by their children.²³ Children are expected to abide by their parents' will,²⁴ lack the opportunity to express their feelings until a certain age,²⁵ and

15. See Lindsay, *supra* note 6.

16. Forty-seven percent of adults have searched for information about themselves online. Mary Madden et al., *Digital Footprints*, PEW RSCH. CTR. (Dec. 16, 2007), <https://www.pewresearch.org/internet/2007/12/16/digital-footprints/> [<https://perma.cc/92E9-EAZ3>].

17. Lindsay, *supra* note 6.

18. See *Pierce v. Soc'y of Sisters*, 268 U.S. 510, 534–35 (1925); *Troxel v. Granville*, 530 U.S. 57, 65 (2000).

19. Meaghann S. Weaver et al., *Honoring the Good Parent Intentions of Courageous Parents: A Thematic Summary from a US-Based National Survey*, 7 CHILD., no. 12, Dec. 1, 2020, at 1–2.

20. See Maja Sonne Damkjaer, *Sharenting = Good Parenting?*, in DIGITAL PARENTING: THE CHALLENGES FOR FAMILIES IN THE DIGITAL AGE 209, 209 (Giovanna Mascheroni et al. eds., 2018), <https://norden.diva-portal.org/smash/get/diva2:1265024/FULLTEXT02.pdf> [<https://perma.cc/MV5V-K4BA>].

21. See Jenn Supple Bartels, *Parents' Growing Pains on Social Media: Modeling Authenticity*, 1 CHARACTER & SOC. MEDIA 51, 63 (2015).

22. See Grace Greene, *Instagram Lookalikes and Celebrity Influencers: Rethinking the Right to Publicity in the Social Media Age*, 168 U. PA. L. REV. ONLINE 153, 186 (2020).

23. See Shannon Sorensen, *Protecting Children's Right to Privacy in the Digital Age: Parents as Trustees of Children's Rights*, 36 CHILD. LEGAL RTS. J. 156, 164 (2016).

24. Stacey Steinberg, *Sharenting: Children's Privacy in The Age of Social Media*, 66 EMORY L.J. 839, 868 (2017).

25. See Jeffrey Shulman, *The Parent as (Mere) Educational Trustee: Whose Education Is It, Anyway?*, 89 NEB. L. REV. 290, 297 (2010).

largely do not understand the implications of their parents' online conduct.²⁶ Generally, online accounts dedicated to sharing photos and videos of children are very successful: W.E., a three-year-old girl, has over sixteen million followers on TikTok.²⁷

Sharenting, a combination of the words "sharing" and "parenting," is a term coined by Wall Street Journal writer Steven Leckart that refers to the practice of oversharing information about one's child on various social media platforms,²⁸ spurred by the "always online" culture. Sharenting, however, is not limited to parents but also includes grandparents, educators, guardians, and other adults entrusted with the responsibility of a child in their homes or their care.²⁹

When parents resort to sharenting, it is often to connect with their community and to seek support.³⁰ Being a parent is a difficult role, and social media offers the support that lonely parents need and the guidance they are seeking. Most parents act with good intentions as they are not aware of the long-term consequences of sharenting.³¹ The average parent lacks the knowledge or skills necessary to protect their children from the potential hazards of sharing PII online.³² Parenting does not come with a "cigarette-style warning label or nutrition-style information label,"³³ and an uninformed parent may end up relinquishing a child's privacy in

26. See Steinberg, *supra* note 24, at 863.

27. Wren & Jacquelyn (@wren.eleanor), TIKTOK, <https://www.tiktok.com/@wren.eleanor?lang=fr> [<https://perma.cc/8EFE-SXK8>].

28. Allison Lichter, *Oversharenting: Parents Juggle Their Kids' Lives Online*, WALL ST. J. (May 16, 2012), https://www.wsj.com/articles/BL-JB-15164?gaa_at=eafs&gaa_n=AWetsqd5KjR8ziIpwiVMavi9K-nW1bF37QTPqMNHY-E4Lxb8IFBqqMvAxvl_drFevr0%3D&gaa_ts=68f5521b&gaa_sig=6hF7iIpJ4hIsN4Mi_RbxB0a4w05QwldluqArwb9cFa0AN3bzNJNaDElmzrorbtMo9G6houblvBD_Vsy-dMf9Xw%3D%3D [<https://perma.cc/S8CN-9E5H>]. Sharenting was added to the list of Scrabble words in 2019. Anita Singh, *New Scrabble Words: Genderqueer, Hackerazzo and Sharenting Added to Dictionary*, TELEGRAPH (May 2, 2019), <https://www.telegraph.co.uk/news/2019/05/02/new-scrabble-words-genderqueer-hackerazzo-sharenting-added-dictionary/> [<https://perma.cc/52EB-TACR>].

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

30. Steinberg, *supra* note 24, at 841–42.

31. *Sharenting Trends: Do Parents Share Too Much About Their Kids on Social Media?*, C.S. MOTT CHILD.'S HOSP. (Mar. 16, 2015), <https://www.mottchildren.org/media/32651> [<https://perma.cc/UU89-NXSL>] (explaining that parents need to be more cognizant of the impact posting about their children on social media could have).

32. Bahareh Ebadifar Keith & Stacey Steinberg, *Parental Sharing on the Internet: Child Privacy in the Age of Social Media and the Pediatrician's Role*, 171 JAMA PEDIATRICS 413, 413 (2017).

33. Leah Plunkett, *To Stop Sharenting & Other Children's Privacy Harms, Start Playing: A Blueprint for a New Protecting the Private Lives of Adolescents and Youth (PPLAY) Act*, 44 SETON HALL LEGIS. J. 457, 461 (2020).

exchange for the sought-after influencer status,³⁴ or simply because they did not know any better.

In most instances, sharenting “[a]t worst [may] be negligent, [but] lawful.”³⁵ However, it is often the case that parents are rewarded by their social network through likes, comments, and shares, resulting in positive stimuli, and incentivizing them to further share online.³⁶ In the process, children’s privacy is forfeited, and the opportunity for them to control their own digital footprints is hindered.³⁷ Leah Plunkett describes sharenting as the default setting for today’s adults.³⁸

Sharenting and its effects have largely gone unaddressed.³⁹ Children have an interest in safeguarding any negative information about themselves that their parents may post on social media, and have the right to disagree with their parent’s decision to broadcast their pictures and day-to-day life to the world.⁴⁰ Minors in the digital age, however, have limited control over the distribution of their PII, which is often determined by their parents and guardians.⁴¹ Unlike adults who can set their privacy parameters when making the conscious decision to share their PII with the world, children are not afforded this privilege.⁴²

Some newborns, toddlers, and teenagers end up with an indelible digital footprint⁴³ that is accessible to anyone around the globe at any time through Google Index, even when the content is taken down.⁴⁴ Simply put, information on the internet is forever.⁴⁵ Disclosures made during childhood on the internet, either by a parent, an acquaintance, or the child herself have the potential to last a lifetime, as information shared

34. Emma Nottingham, ‘Dad! Cut that Part Out!’ *Children’s Rights to Privacy in the Age of ‘Generation Tagged’: Sharenting, Digital Kidnapping and the Child Micro-Celebrity*, in THE ROUTLEDGE INT’L HANDBOOK OF YOUNG CHILD.’S RTS. 183, 189 (Jane Murray et al. eds., 2019). An influencer is “a person who is paid by a company to show and describe its products and services on social media, encouraging other people to buy them.” *Influencer*, CAMBRIDGE ENG. DICTIONARY, <https://dictionary.cambridge.org/us/dictionary/english/influencer> [<https://perma.cc/9XAX-XP6N>].

35. PLUNKETT, *supra* note 29, at xvii.

36. See Mary Bowerman, *Do You Overshare About Your Kids Online?*, USA TODAY (Mar. 16, 2015), <https://www.usatoday.com/story/tech/2015/03/16/parents-over-sharing-online/24825981/> [<https://perma.cc/2CAZ-LP5P>].

37. See Steinberg, *supra* note 24, at 839.

38. See PLUNKETT, *supra* note 29, at xv–xvi.

39. Benjamin Shmueli & Ayelet Blecher-Prigat, *Privacy for Children*, 42 COLUM. HUM. RTS. L. REV. 759, 763 (2011).

40. *Id.*

41. Steinberg, *supra* note 24, at 843–44.

42. *Id.* at 843.

43. *Id.* at 844 n.21 (explaining why digital footprints are indelible).

44. See *View Webpages Cached in Google Search Results*, GOOGLE, <https://support.google.com/websearch/answer/1687222?hl=en> [<https://perma.cc/6QCU-X829>].

45. See *id.*

online can persist long after its relevance has diminished.⁴⁶ The child's digital footprint can spiral out of control and become unmanageable as every detail about their life becomes entertainment for adults to consume: a detailed day in the life vlog, outfit of the day videos, and even documented birthday celebrations.

As these kids grow older, the potential for emotional and psychological harm is significant once they understand the extent of what has been shared about their childhood online.⁴⁷ Twenty-five percent of surveyed children expressed to CBBC Newsround that they feel "embarrassed," "anxious," and "worried" when their parents share content about them on social media platforms.⁴⁸ The stigmas that children may have been subjected to during their unwanted time as social media "stars" could potentially haunt them for the rest of their lives, even as they grow up and try to distance themselves from that part of their past.⁴⁹

However, the most serious problem arises when sharented content falls into the hands of pedophiles or people with pedophilic tendencies. According to the head of Canada's Online Child Photography Tip Line, images of children doing "normal things" are often shared on pedophile websites.⁵⁰ Pedophiles and people with pedophilic tendencies often scour social media platforms in search of accounts where parents overshare information and images of their children.⁵¹ They may use hashtags, keywords, or location data to find these accounts.⁵² Once predators have identified a target, they may begin to save or download the images for their personal use or share them on pedophile websites and databases.⁵³ Unfortunately, once an image has been sourced from the internet and shared on one of these platforms, it can be nearly impossible to remove

46. See Agnieszka A. McPeak, *The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery of Social Media Data*, 48 WAKE FOREST L. REV. 887, 899 (2013).

47. Nottingham, *supra* note 34, at 186.

48. *Sharenting: Are You OK with What Your Parents Post?*, BBC (Feb. 7, 2017), <https://www.bbc.co.uk/newsround/38841469> [<https://perma.cc/6SS7-NWTG>].

49. *Id.*

50. Sharon Kirkey, *Do You Know Where Your Child's Image Is? Pedophiles Sharing Photos from Parents' Social Media Accounts*, NAT'L POST (Apr. 18, 2017), <https://nationalpost.com/news/canada/photos-shared-on-pedophile-sites-taken-from-parents-social-media-accounts> [<https://perma.cc/87BW-3653>].

51. See Chris McKenna, *4 Ways Pedophiles Exploit Instagram to Groom Kids*, PROTECT YOUNG EYES (Apr. 19, 2019), <https://protectyouneyes.com/4-ways-pedophiles-exploit-instagram-groom-kids/> [<https://perma.cc/43EH-A42S>].

52. *Id.*

53. See Roderic Broadhurst & Matthew Ball, *How the World's Biggest Dark Web Platform Spreads Millions of Items of Child Sex Abuse Material—And Why It's Hard To Stop*, THE CONVERSATION (Sept. 2, 2021), <https://theconversation.com/how-the-worlds-biggest-dark-web-platform-spreads-millions-of-items-of-child-sex-abuse-material-and-why-its-hard-to-stop-167107> [<https://perma.cc/8F6S-UP7L>].

completely from the dark web due to the complexity and anonymity of pedophile networks.⁵⁴

B. *Facts and Figures: The Hidden Realities of Sharenting*

Long before the rise of social media as we know it today, researchers warned of the proliferation of child pornography online due to the frequent usage of the internet by sexual predators.⁵⁵ According to InHope—a network of forty-seven cyber tip lines—during the pandemic, reports of online child sexual exploitation activity to cyber tip hotlines rose by thirty percent globally.⁵⁶ In the United States, the National Center for Missing and Exploited Children (NCMEC) counted 983,734 reports in 2019, and almost double that number, 2,027,520 reports in 2020.⁵⁷ The NCMEC expressed that a considerable chunk of the reports concern short videos that went viral on social media.⁵⁸

Other child safety experts and law enforcement officials have reported that distributors of child sexual abuse images use coded language to avoid detection by the safety tools of social media companies such as YouTube, Facebook, Twitter, and Instagram; private messaging applications such as Telegram and WhatsApp; and file-sharing sites such as Mega.⁵⁹ As pedophiles trade links to material in plain sight on these platforms, they use coded terms such as “C.P.,” referring to “child pornography,” and “caldo de pollo,” which is Spanish for “chicken soup.”⁶⁰

Some parents are of the impression that by sharing images or videos of their children on one social media platform, only a select audience will be able to access the content.⁶¹ Facebook, for example, allows users to choose a specific audience for each piece of content,⁶² but in reality, posts can reach a larger group when the intended audience saves and reposts the content on alternate social media platforms.⁶³ For example, if a parent decides to post an innocent image of their toddler daughter on Facebook

54. *Id.*

55. See MONIQUE MATTEI FERRARO & EOGHAN CASEY, INVESTIGATION CHILD EXPLOITATION AND PORNOGRAPHY: THE INTERNET, THE LAW AND FORENSIC SCIENCE 46–47 (Mark Listewink et al. eds., 2005).

56. Olivia Solon, *Child Sexual Abuse Images and Online Exploitation Surge During Pandemic*, NBC NEWS (Apr. 23, 2020), <https://www.nbcnews.com/tech/tech-news/child-sexual-abuse-images-online-exploitation-surge-during-pandemic-n1190506> [https://perma.cc/5RKL-FAZ5].

57. *Id.*

58. *Id.*

59. *Id.*

60. *Id.*

61. Steinberg, *supra* note 24, at 850.

62. Agnieszka McPeak, *Social Media Snooping and Its Ethical Bounds*, 46 ARIZ. ST. L.J. 845, 899–900 (2014).

63. *Id.* at 901.

and adjusts the sharing parameters to “friends of friends,” strangers would be allowed to re-share the image to their respective circles. Things can spiral out of control quickly as the circles grow, which is often an unintended consequence of sharenting on social media. With each subsequent share of sharented content, the probability of its dissemination into the social media feeds of potential predators increases, heightening the need for vigilance and caution in the online sharing of PII.

Regardless, a study done by the Pew Research Center showed that 88% of parents surveyed said they feel comfortable when content is posted about their children on social media.⁶⁴ But, a study by the C.S. Mott Children’s Hospital reports that 74% of the parents surveyed know of at least one other parent who shared “too much” information about a child online, and 67% were concerned that someone would share their child’s PII on another social media channel.⁶⁵ Similarly, another study highlights that 61% of surveyed mothers admitted that posting pictures or comments about their children was their most frequent Facebook activity.⁶⁶

In the United States, 92% of two-year-olds have an online presence, of which 33% have appeared on social media when they were newborn babies.⁶⁷ The pervasive presence of social media in modern society has contributed to this staggering statistic, which may be attributed to a combination of factors, such as the desire to document and share important moments in a child’s life, the need for social validation, and the influence of cultural norms surrounding technology usage.

On Facebook, 45% of posts that have a child’s image will also mention their name, and 6% will mention their date of birth.⁶⁸ On Instagram, 63% of parents reference their children’s name in at least one photo on their profile and 27% will reference their children’s date of birth.⁶⁹ According to a recent study, videos that include a child under the

64. Maeve Duggan et al., *Parents and Social Media*, PEW RSCH. CTR. (July 16, 2015), <https://www.pewresearch.org/internet/2015/07/16/main-findings-14/> [https://perma.cc/KNW6-TE4E].

65. C.S. Mott Child.’s Hosp., *Parents on Social Media: Likes and Dislikes of Sharenting*, 23 NAT’L POLL ON CHILD.’S HEALTH, no. 2, Mar. 16, 2015, at 1, https://mottpoll.org/sites/default/files/documents/031615_sharenting_0.pdf [https://perma.cc/QB6Y-KW2M].

66. Charlotte Chalklen & Heather Anderson, *Mothering on Facebook: Exploring the Privacy/Openness Paradox*, SOC. MEDIA & SOC’Y, no. 2, May 17, 2017, at 7.

67. Tim Stevens, *Study Finds 92% of Kids Are Online by Age 2, Baby Dating Site Valuations Soar*, ENGADGET (Oct. 8, 2010), <https://www.engadget.com/2010-10-08-study-finds-92-of-kids-are-online-by-age-2-baby-dating-site-va.html> [https://perma.cc/FG3Y-6TCT].

68. Tehila Minkus et al., *Children Seen but Not Heard: When Parents Compromise Children’s Online Privacy*, in PROCS. OF THE 24TH INT’L CONF. ON WORLD WIDE WEB 776, 779 (2015), <https://cse.engineering.nyu.edu/~tehila/pubs/WWW2015children.pdf> [https://perma.cc/C6LL-XUN2].

69. *Id.* at 783.

age of thirteen get three times more views than those that do not have children.⁷⁰

According to the Australian Children's eSafety Commissioner, roughly half of the images found on a dark website that shares pedophilic content—containing at least forty-five million images—were sourced from social media platforms and family blogs.⁷¹ Folders on these websites were labeled “Facebook,” “Kik girls,” and “my daughter's Instagram friends.”⁷² This number, although shocking, is a sobering reminder of the dark side of the digital age. This unsettling statistic raises important questions about the mechanisms by which content is disseminated and ultimately finds its way onto the dark web where it is often traded, and how it is consumed by individuals with malicious intentions.

II. THE DISTURBING WORLD OF CHILD PORNOGRAPHY: AN EXAMINATION OF ITS FORMS AND TYPES

The effects of sharenting become palpable whenever unintended third-party recipients acquire the sharented information. A significant portion of the pornographic and abusive images of children found online are created from real photos that are manipulated and turned into illicit content by malicious individuals on the dark web.⁷³ As such, the nature of the material that is subsequently reshared can be broadly classified into three distinct categories: real, virtual, or morphed child pornography. The distinction between these categories is predicated on the unique characteristics of each type of material, which not only carries different legal implications, but also reflects ethical considerations.

A. *Real Child Pornography*

In 1977, Congress passed the Protection of Children against Sexual Exploitation Act, criminalizing the use of a minor in obscene depictions of sexually explicit conduct.⁷⁴ Before that, laws against child

70. Patrick Van Kessel et al., *A Week in the Life of Popular YouTube Channels*, PEW RSCH. CTR. (July 25, 2019), <https://www.pewresearch.org/internet/2019/07/25/a-week-in-the-life-of-popular-youtube-channels/> [https://perma.cc/V3B6-DZAZ].

71. Lucy Battersby, *Millions of Social Media Photos Found on Child Exploitation Sharing Sites*, SYDNEY MORNING HERALD (Sept. 30, 2015), <http://www.smh.com.au/national/millions-of-social-mediaphotos-found-on-child-exploitation-sharing-sites-20150929-gixe55.html> [https://perma.cc/APW6-VUMA].

72. *Id.*

73. Plunkett, *supra* note 33, at 468.

74. Protection of Children against Sexual Exploitation Act of 1977, Pub. L. No. 95-225, 92 Stat. 7.

pornography were virtually non-existent in the United States.⁷⁵ Then, in 1984, Congress passed the Child Protection Act, which outlawed the distribution of material depicting the sexual exploitation of minors, regardless of whether the material was deemed obscene or not.⁷⁶ Later, in 1986, the Child Sexual Abuse and Pornography Act made it a federal criminal offense for anyone to advertise a product depicting sexually explicit conduct with a minor or the opportunity to engage in such conduct with a minor.⁷⁷ Before the adoption of these laws, the obscenity of images depicting minors was determined by common law standards that balanced the nature of the image with First Amendment rights.

In *Miller v. California*, the U.S. Supreme Court established the three-part *Miller* test for determining whether material is obscene, and therefore, not protected by the First Amendment to the U.S. Constitution.⁷⁸ The *Miller* test required that the average person, applying contemporary community standards, would find that the work, taken as a whole, appeals to the prurient interest; depicts or describes, in a patently offensive way, sexual conduct specifically defined by applicable state law; and lacks serious literary, artistic, political, or scientific value.⁷⁹

In *New York v. Ferber*, the U.S. Supreme Court upheld a New York law prohibiting the distribution of child pornography that did not meet the obscenity standard and established the child pornography exception to the First Amendment using the strict scrutiny test.⁸⁰ The defendant, Paul Ferber, was convicted for selling a film depicting underage boys masturbating to an undercover police officer.⁸¹ In its decision, the Court held that child pornography was not entitled to First Amendment protection because it was not a form of expression that had any social value.⁸²

Then, in *Osborne v. Ohio*, the Supreme Court expanded the child pornography exception to the First Amendment, permitting states to criminalize the possession of child pornography.⁸³ Charles Keith Osborne was found in possession of images of nude adolescent boys in “sexually explicit positions,” and was charged with violating the Ohio law.⁸⁴ In its

75. Artemus Ward, *Child Pornography*, THE FIRST AMENDMENT ENCYCLOPEDIA (2009), <https://www.mtsu.edu/first-amendment/article/993/child-pornography> [<https://perma.cc/NW8B-H6ZG>].

76. *See id.*; Child Protection Act of 1984, Pub. L. No. 98-292, 98 Stat. 204.

77. *See* Ward, *supra* note 75; Child Sexual Abuse and Pornography Act of 1986, Pub. L. No. 99-628, 100 Stat. 3510.

78. *Miller v. California*, 413 U.S. 15, 24 (1973).

79. *Id.*

80. *New York v. Ferber*, 458 U.S. 747, 756 (1982).

81. *Id.* at 752.

82. *Id.* at 775.

83. *Osborne v. Ohio*, 495 U.S. 103, 103 (1990).

84. *Id.*

decision, the Court recognized that the possession of child pornography contributed to the creation and distribution of such materials, which in turn led to the exploitation of children.⁸⁵

Federal laws criminalizing child pornography are codified in Title 18 of the United States Code. Child pornography is defined as any visual depiction of sexually explicit conduct involving a minor.⁸⁶ Currently, 18 U.S.C. § 2251 concerns the “Sexual exploitation of children” and encompasses the production of child pornography. 18 U.S.C. § 2252 criminalizes “certain activities relating to material involving the sexual exploitation of minors” which includes the possession, distribution, and receipt of child pornography if it affects any means or facility of interstate or foreign commerce.⁸⁷

B. *Virtual Child Pornography*

In 1996, as pedophiles were finding creative ways to depict children in sexual ways, and as a response to *Osborne*, Congress enacted the Child Pornography Prevention Act (CPPA).⁸⁸ Through the CPPA, Congress wanted to broaden the definition of child pornography to include “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture” that is or appears to be of “a minor engaging in sexually explicit conduct,”⁸⁹ and any sexually explicit image that is “advertised, promoted, presented, described, or distributed in such a manner that conveys the impression” it depicts “a minor engaging in sexually explicit conduct.”⁹⁰ Specifically, Congress wanted to criminalize computer-generated content that depicts minors engaging in sexually explicit conduct, commonly known as virtual child pornography. Virtual child pornography are sexually explicit images “created by using adults who look like minors or by using computer imaging.”⁹¹

However, the Free Speech Coalition challenged the constitutionality of the CPPA because, under the new law, images that do not depict actual children could be considered child pornography.⁹² The Supreme Court in *Ashcroft v. Free Speech Coalition* held that the language of the CPPA was too broad, and violated the First Amendment because it prohibited a wide range of constitutionally protected speech, including speech that did

85. *Id.* at 125.

86. 18 U.S.C. § 2256.

87. *See* 18 U.S.C. §§ 2251, 2252, 2252A.

88. 18 U.S.C. § 2252A.

89. 18 U.S.C. § 2256(8)(B).

90. 18 U.S.C. § 2256(8)(D) (repealed 2003).

91. *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 267 (2002).

92. *Id.*

not involve real children.⁹³ The Court also noted that the statute would chill legitimate speech, such as artistic expression, and could lead to arbitrary and discriminatory enforcement.⁹⁴ *Ashcroft* remains good law, and virtual child pornography is legal in the United States.⁹⁵

C. Morphed Child Pornography

Although the Court in *Ashcroft* ruled the CPPA unconstitutional, it refrained from commenting on the legality of morphed child pornography,⁹⁶ and therefore created a grey area in the law.⁹⁷ Professor Stacey Steinberg explains that morphed child pornography involves the combination of an “innocent” image of a minor, with the sexual image of an adult, created with morphing software.⁹⁸ Unlike virtual child pornography, morphing requires the use of the image of a real child, but, similar to virtual child pornography, no child is engaged in sexually explicit conduct.⁹⁹ Often, the “innocent images” originate from social media¹⁰⁰ when shared content is viewed by a pedophile or someone with pedophilic tendencies.¹⁰¹ Pictures of children in any state of undress, specifically images of potty training or bath time, are popular content on predatory websites.¹⁰²

For those reasons, Congress enacted the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act (PROTECT) of 2003, which criminalizes conduct that knowingly “advertises, promotes, presents, distributes, or solicits . . . any material or purported material in a manner that reflects the belief, or that is intended to cause another to believe [it is] . . . an obscene visual depiction of a minor engaging in sexually explicit conduct.”¹⁰³ Under the PROTECT Act, states no longer needed to prove that a defendant ever possessed, created, received, or distributed an image depicting real child pornography in the context of morphed child pornography.¹⁰⁴

93. *Id.* at 258.

94. *Id.*

95. *United States v. Mecham*, 950 F.3d 257, 269 (5th Cir. 2020).

96. *Ashcroft*, 535 U.S. at 242 (finding “respondents [did] not challenge” the provision that the images fell “within the definition of virtual child pornography” and thus the Court need not consider the issue).

97. Steinberg, *supra* note 24, at 903.

98. *Id.* at 911.

99. *Mecham*, 950 F.3d at 260.

100. Kirkey, *supra* note 50.

101. *Id.*

102. Steinberg, *supra* note 24, at 847.

103. Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003, Pub. L. No. 108-21, 117 Stat. 650 (codified as amended in scattered sections of 18 U.S.C.).

104. *See United States v. Williams*, 553 U.S. 285, 293 (2008).

In *United States v. Mecham*, the Fifth Circuit upheld the defendant's conviction for morphed child pornography for adding the faces of his four granddaughters to photos and videos of adults engaged in sexual conduct.¹⁰⁵ Mecham possessed over 30,000 pornographic files,¹⁰⁶ and he often morphed his face onto the face of the men engaging in sexual acts.¹⁰⁷ Mecham was denied certiorari by the U.S. Supreme Court in June 2020.¹⁰⁸

In *United States v. Hotaling*, the defendant morphed the faces of six minor girls onto the bodies of nude and partially nude adult females engaged in sexually explicit conduct.¹⁰⁹ Some of the images depicted sadistic or masochistic scenes where the morphed minors were restrained by handcuffs, dog collars, and leashes.¹¹⁰ The Second Circuit affirmed the district court's decision that morphed child pornography is not protected speech under the First Amendment.¹¹¹

In *Doe v. Boland*, the defendant was a technology expert and lawyer who testified in another case to help his client resist child pornography charges.¹¹² He downloaded images of children from a stock photography website and used morphing technology to superimpose the children's faces onto the bodies of adults engaged in sexual activities, to prove that his client might not have known that they were viewing child pornography.¹¹³ When the parents of the children discovered the images, they sued Boland under two federal child pornography laws. The Sixth Circuit affirmed the district court's summary judgment decision and upheld the \$300,000 damages award to the plaintiffs.

Multiple United States Courts of Appeals have held that the PROTECT Act's categorical ban on morphed child pornography is constitutional,¹¹⁴ but the U.S. Supreme Court has yet to take on a case challenging the illegality of morphed child pornography or the effects of sharenting.¹¹⁵ Professor Steinberg believes that "the Court should find that this future harm to a potential child, coupled with the circulation

105. *Mecham*, 950 F.3d at 258.

106. *Id.*

107. *Id.* at 259.

108. *Mecham v. United States*, 141 S. Ct. 139 (2020).

109. *United States v. Hotaling*, 634 F.3d 725, 727 (2d Cir. 2011).

110. *Id.*

111. *Id.*

112. *Doe v. Boland*, 698 F.3d 877, 879 (6th Cir. 2012).

113. *Id.*

114. *See Mecham*, 950 F.3d at 258; *Hotaling*, 634 F.3d at 727; *Boland*, 698 F.3d at 879; *United States v. Bach*, 400 F.3d 622, 632 (8th Cir. 2005).

115. In *United States v. Williams*, the Supreme Court held that section 2252A(a)(3)(B) of the PROTECT Act, which criminalizes the pandering or solicitation of child pornography, is constitutional. However, the court did not comment on the constitutionality of morphed child pornography. 553 U.S. 285, 293.

harm to an actual child, is significant enough to warrant morphed child pornography's exclusion from the protections of the First Amendment."¹¹⁶

III. THE INCREASING GAP BETWEEN TECHNOLOGY AND THE LAW IN THE UNITED STATES: CHALLENGES FOR THE COURTS

Deciding on the appropriate legal framework to apply in cases where the competing interests of parents' right to care, custody, and control over their children, and the child's right to privacy clash is a daunting task. This is because both interests are constitutionally protected,¹¹⁷ and balancing them requires a nuanced analysis of the unique facts and circumstances of each case, as well as a deep understanding of the relevant statutory and case law. Furthermore, the complexity and ambiguity inherent in these legal frameworks can make the decision-making process even more intricate, requiring an astute evaluation of legal precedents and often, a moral and ethical judgment.

A. *The Haunting Shadow of Sidis*

When it comes to decisions about raising their children and directing their upbringing, parents enjoy a constitutionally protected liberty interest,¹¹⁸ but they are bound by child welfare laws: parents cannot subject their children to abuse, neglect, or the manufacturing of child pornography.¹¹⁹ However, considering the circumstances of family life, courts are generally reluctant to grant children privacy rights.¹²⁰ The parent's interest in exercising control over the minor often trumps the child's reasonable expectation of privacy.¹²¹ In the context of sharenting, decisions about "whether," "why," "with whom," "how," and "when to sharent" fall within the discretion of adults.¹²²

116. Steinberg, *supra* note 24, at 930.

117. U.S. Const. amend. XIV. In *Troxel v. Granville*, the U.S. Supreme Court stated that "the interest of parents in the care, custody, and control of their children--is perhaps the oldest of the fundamental liberty interests recognized by this Court." 530 U.S. 57, 65.

118. *Id.*

119. PLUNKETT, *supra* note 29, at 474.

120. David D. Meyer, *The Modest Promise of Children's Relationship Rights*, 11 WM. & MARY BILL RTS. J. 1117, 1118 (2003).

121. *Id.* at 1117–18; *Nguon v. Wolf*, 517 F. Supp. 2d 1177, 1183, 1193–94 (C.D. Cal. 2007) (holding that a school's right to follow due process (that results in the school telling parents about their child's sexual orientation) outweighed the child's privacy right); *Pierce v. Soc'y of Sisters*, 268 U.S. 510, 534–35 (1925) (overturning a law requiring public education for all students, resting its decision on the parent's interest, rather than the child's liberty interest); *Shields v. Gross*, 448 N.E.2d 108, 112 (N.Y. Ct. App. 1983) (holding that a minor may not disaffirm written consent given by their parent for the use of their "name, portrait or picture for advertising purposes.").

122. PLUNKETT, *supra* note 29, at 474.

Twenty years before the development of the internet, in *Sidis v. F-R Publishing*, the United States Court of Appeals for the Second Circuit ruled that if a person was in the public spotlight as a child, they would remain a public figure for the rest of their life.¹²³ William James Sidis was a child prodigy and received national public attention in 1910 for lecturing to distinguished mathematicians on the subject of four-dimensional bodies.¹²⁴ However, Sidis did not want to remain in the public eye as an adult and went to great lengths to protect his privacy and live a secluded life.¹²⁵ Despite his dislike of media attention, the *New Yorker* published a story about Sidis' life, where intimate details about the prodigy were shared.¹²⁶ Shortly after the piece was published, Sidis sued the *New Yorker* alleging that the company violated his right to privacy.¹²⁷ The court disagreed, holding that since Sidis was a public figure as a child, the general public has a legitimate interest in the story published by *The New Yorker*.¹²⁸ While Sidis has an interest in privacy, the public also has an interest in knowing about his life.¹²⁹ The court stated that while there may be some circumstances where the unauthorized use of a person's name or likeness could give rise to an actionable claim for invasion of privacy, such claims must be balanced against the First Amendment's guarantee of free speech and the public's interest in access to information.

Since this case remains good law, it can be argued that if a parent leads their child to internet fame through sharenting, the child would forever be subject to privacy laws governing public figures.¹³⁰ In other terms, parents' actions have the power to limit or jeopardize a future adult's right to privacy.

B. *The COPPA's Inability to Protect Children*

In 1998, Congress enacted the Children's Online Privacy Protection Act (COPPA) as a response to the increasing number of children accessing the internet.¹³¹ COPPA applies to operators of commercial websites for kids and websites that operate with "actual knowledge" that

123. *Sidis v. F-R Publ'g*, 113 F.2d 806, 809 (2d Cir. 1940).

124. *Id.* at 807.

125. *Id.*

126. *Id.*

127. *Id.*

128. *Sidis*, 113 F.2d at 809.

129. *Id.*

130. *Id.* at 808; Steinberg, *supra* note 24, at 860.

131. Children's Online Privacy Protection Act, 15 U.S.C. § 6502.

they are collecting, using, or disclosing PII¹³² from children under the age of thirteen.¹³³

Operators must post on their websites a privacy policy, obtain verifiable parental consent before collecting, using, or disclosing a child's PII, maintain the confidentiality of the PII, and provide parents the right to delete the child's PII.¹³⁴ In addition, website operators have to destroy the child's PII after fulfillment of the intended business purpose.¹³⁵ Any business that violates the terms of COPPA may be liable for civil penalties of up to \$43,280 per violation through the Federal Trade Commission's (FTC) enforcement mechanisms.¹³⁶ Since the benefit of harboring children's PII exceeds the monetary fines imposed by the FTC, COPPA penalties remain another "cost of doing business."¹³⁷

However, COPPA protects information collected *from* children, rather than information collected *about* children, and PII posted by a child's parent does not receive COPPA protection.¹³⁸ As Leah Plunkett puts it, "Limiting privacy protection to PII that comes directly from kids of any age leaves a vast amount of information about kids unprotected by COPPA."¹³⁹

While COPPA provides some safeguards for children's online privacy, and despite its good intentions, it does not address the potential harm that can arise from the sharenting of children's PII and images. As a result, there is no federal law in the United States that limits the online behavior of parents or other adults to safeguard the privacy of children.¹⁴⁰

132. Personal information includes (but is not limited to) an individual's name, address, cookies, Internet Protocol addresses, and device serial number. *See* 16 C.F.R. § 312.2 (2024).

133. *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N § A(1) (July 2020), <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0> [<https://perma.cc/9C9K-BN5V>]; 16 C.F.R. § 312.3 (2024).

134. *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N § A(1) (July 2020), <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0> [<https://perma.cc/9C9K-BN5V>].

135. *Id.*

136. *Id.* § B(2). In 2015, the FTC imposed a \$5 billion penalty on Facebook (now Meta) for violating a privacy order. *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019), <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions> [<https://perma.cc/2YTJ-G684>].

137. Eldar Haber, *Toying with Privacy: Regulating the Internet of Toys*, 80 OHIO ST. L.J. 399, 441–42 (2019).

138. *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N § A(8) (July 2020), <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0> [<https://perma.cc/9C9K-BN5V>]. *See* 16 C.F.R. §§ 312.2–312.3 (2024).

139. PLUNKETT, *supra* note 29, at 475.

140. *See generally* Keith & Steinberg, *supra* note 32.

Similarly, no law gives children the right to take legal action in case of harm.¹⁴¹

C. *The Uphill Legal Battle*

Cases of sharenting leading to children's harm are not common in the United States.¹⁴² This is because, first, most sharenting is innocent, meaning that parents share everyday images of their children with their limited circle on social media and do not intend for any harm to happen.¹⁴³ Second, there is no federal law in the United States that allows any affected party to sue an adult for any harm that resulted from sharenting.¹⁴⁴ By contrast, a Dutch court used the European General Data Protection Regulation (GDPR) to ban a grandmother from posting photos of her grandchildren online without parental consent.¹⁴⁵ The GDPR prohibits the processing of children's PII without parental consent.¹⁴⁶ In its decision, the Dutch court highlighted that the defendant's privacy settings were not successfully established, meaning that it was unclear whether the children's images could be found through a search engine.¹⁴⁷

In 2016, a Zambian woman was looking after a couple's child in Maryland when she took prosaic photographs of the minor and proceeded to post them on Facebook.¹⁴⁸ In court, the parents alleged that the woman had infringed on the parent's right to privacy by publishing their minor child's images on social media.¹⁴⁹ The district court did not agree, stating

141. Some state laws protect children from abuse inflicted by parents, including emotional harm whereby a state could seek a remedy through the dependency court, or obtain injunctive relief that precludes the parent from posting additional content that harms the child online. However, children have little to no control over these lawsuits since state actors are the holders of the right to bring forth litigation. In addition, these lawsuits are likely to fail if argued from a censorship standpoint due to the prior restraints doctrine. Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 344 (2005).

142. When running a search for the word "sharenting," and limiting the results to cases, only one result was generated by LexisPlus on May 1, 2023. *Grossman v. Rockaway Twp.* is a case that does not address sharenting and its effects, but the Superior Court of New Jersey referenced a sharenting scholar in its discussion, which triggered the result. No MRS-L-1173-18, 2019 WL 2649153, at *2 (N.J. Super. Ct. June 10, 2019).

143. See discussion *supra* Section I.A.

144. See discussion *supra* Section III.B.

145. Stacey Steinberg, *An Oversharing Grandma's Court Case Offers Lessons On Setting Boundaries For Kids' Online Privacy*, WASH. POST (Mar. 27, 2020), <https://www.washingtonpost.com/lifestyle/2020/05/27/an-oversharing-grandmas-court-case-offers-lessons-setting-boundaries-kids-online-privacy/> [<https://perma.cc/4S23-ZJGD>].

146. *Id.*

147. *Id.*

148. *Sakala v. Milunga*, No. PWG-16-790, 2017 WL 2986364, at *1 (D. Md. July 13, 2017).

149. *Id.* at *4.

the parents failed to allege essential elements,¹⁵⁰ which highlights how child privacy laws are not tailored to the digital age in the United States.

In *Thomas v. Cash*, the adoptive parents of a child requested an order of protection against the biological family for sharing pictures of the minor on their Facebook accounts.¹⁵¹ The appellate court lifted the protective order granted by the trial judge, explaining that the adoptive parents caused the invasion of their child's privacy.¹⁵² The court reasoned that because they posted photographs of their minor on Facebook, it is permissible for a stranger to download these images and post them on their own social media accounts.¹⁵³

After a comprehensive analysis of the relevant case law, it remains uncertain how a U.S. court would approach the issue of sharenting in cases where a minor has suffered harm, and how the court would strike a balance between the interest of parents in the care, custody, and control of their children on one hand¹⁵⁴ and the child's digital right to privacy on the other hand.

D. *The National Center for Missing and Exploited Children*

The NCMEC operates a program called "Take It Down" designed to help remove nude and partially nude images and videos of children from the internet.¹⁵⁵ Its goal is to reduce the amount of child sexual abuse material available online and to help protect children from further victimization.¹⁵⁶

Persons wishing to benefit from the service should upload to NCMEC the content they wish to have taken down from the internet.¹⁵⁷ Take It Down generates a hash that is used to identify exact copies of the content online.¹⁵⁸ Then, if an online platform partnering with NCMEC detects the content on its public or unencrypted service, the content will be taken down immediately.¹⁵⁹ NCMEC currently partners with Facebook, Instagram, PornHub, OnlyFans, Yubo, and TikTok.¹⁶⁰

150. *Id.*

151. *Thomas v. Cash*, 423 P.3d 670, 672 (Okla. Civ. App. 2016).

152. *Id.* at 676.

153. *Id.* at 677.

154. *See, e.g., Troxel v. Granville*, 530 U.S. 57, 65 (2019).

155. *Take It Down*, NAT'L CTR. FOR MISSING & EXPLOITED CHILD., <https://takeitdown.ncmec.org> [<https://perma.cc/S4K5-FC3J>].

156. *Id.*

157. *Id.*

158. *Id.*

159. *Id.*

160. *Participating Online Platforms*, NAT'L CTR. FOR MISSING & EXPLOITED CHILD., <https://takeitdown.ncmec.org/participants/> [<https://perma.cc/QS5Q-5989>].

The service is free of charge, anonymous, and open to people from all around the world, as long as the content was created before the child turned eighteen.¹⁶¹

IV. INTERNATIONAL HUMAN RIGHTS LAW, SHARENTING, AND DIGITAL PRIVACY

A singular, unified, international legal instrument limiting sharenting online does not exist. This absence underscores a broader challenge in harmonizing global legal standards, particularly in the realm of digital privacy and the protection of children. The complexity of digital rights, coupled with the sovereignty of nations and their diverse legal systems, makes the establishment of a universally binding law a formidable task. The concept of sharenting touches on various legal and ethical issues, including privacy, consent, and the rights of the child. International legal frameworks, such as the United Nations Convention on the Rights of the Child (CRC), offer broad protections for the rights and well-being of children, including aspects related to privacy.¹⁶² While these provisions are relevant to concerns raised by sharenting, they do not specifically address the practice. Instead, they establish general principles that could and should be interpreted to apply to the digital environment and the sharing of personal information about children.

A. *The Convention on the Rights of the Child*

The United Nations Convention on the Rights of the Child, adopted on November 20, 1989 and entering into force on September 2, 1990, is a comprehensive human rights treaty focusing on the rights and welfare of children worldwide.¹⁶³ It is the most widely ratified international human rights treaty, setting out civil, political, economic, social, and cultural rights for children.¹⁶⁴ Among its various provisions, the CRC emphasizes the right to privacy for children under Article 16, stating that no child shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence, nor to unlawful attacks on their honor and reputation.¹⁶⁵ The CRC's application to the digital environment, while not explicitly mentioned, is increasingly recognized, considering the evolving nature of technology and its impact on children's lives.

161. *Take It Down*, NAT'L CTR. FOR MISSING & EXPLOITED CHILD., <https://takeitdown.ncmec.org> [<https://perma.cc/S4K5-FC3J>].

162. Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.

163. *Id.*

164. *Convention on the Rights of the Child*, UNICEF, <https://www.unicef.org/child-rights-convention> [<https://perma.cc/7HSB-73GX>].

165. Convention on the Rights of the Child, *supra* note 162, at 49.

Critically, the Committee on the Rights of the Child, which oversees the implementation of the CRC, issued General Comment No. 25 on children's rights in relation to the digital environment.¹⁶⁶ This document underscores the importance of protecting children's privacy online, highlighting the need for states to ensure domestic legislation is in place to protect children from arbitrary or unlawful data collection, processing, and dissemination, which aligns with the principles set out in the CRC.¹⁶⁷ The General Comment explicitly acknowledges the challenges and risks that the digital environment poses to children's rights and calls for comprehensive measures to ensure their protection online, reflecting a broad interpretation of the CRC's provisions in the context of modern technology.

B. *The International Covenant on Civil and Political Rights*

The International Covenant on Civil and Political Rights (ICCPR) is a key international treaty that was adopted by the United Nations General Assembly on December 16, 1966, and came into force on March 23, 1976.¹⁶⁸ It is designed to ensure the protection of civil and political rights, including the right to privacy as enshrined in Article 17.¹⁶⁹ It explicitly states that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence, nor to unlawful attacks on their honor and reputation, and that everyone has the right to the protection of the law against such interference or attacks.¹⁷⁰

In General Comment No. 16 on the right to privacy, the Human Rights Committee elaborated on the obligations of states to protect individuals against unlawful or arbitrary interference with their privacy.¹⁷¹ However, the Human Rights Committee has yet to expand the scope of Article 17 to the digital sphere, leaving the protection of digital privacy to domestic legislation.

C. *The Council of Europe's Convention on Cybercrime*

The Council of Europe's Convention on Cybercrime, also known as the Budapest Convention, is a pioneering international treaty that seeks to address internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among

166. Comm. on the Rts. of the Child, Gen. Comment No. 25 on Child.'s Rts. in Relation to the Digit. Env't, U.N. Doc. CRC/C/GC/25 (Mar. 4, 2021).

167. *Id.*

168. International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.

169. *Id.* at 177.

170. *Id.*

171. Human Rights Comm., Gen. Comment No. 16, art. 17 (Apr. 8, 1988), <https://www.refworld.org/legal/general/hrc/1988/en/27539>.

nations.¹⁷² Adopted on November 23, 2001, in Budapest, Hungary, and entering into force on July 1, 2004, the Budapest Convention stands as the first and one of the most significant international legal frameworks specifically designed to combat cybercrime.¹⁷³ It covers a broad range of criminal activities, including offenses related to computer systems, data interference, and content-related offenses, thereby laying a foundation for protecting individuals, including children, in the digital environment.¹⁷⁴

Regarding the protection of children online, the Budapest Convention does not exclusively focus on children but provides several mechanisms that indirectly contribute to their safety. The Convention's provisions on content-related offenses and the criminalization of certain acts, such as child pornography, directly relate to the protection of children in cyberspace.¹⁷⁵ By defining child pornography and mandating its criminalization, the Convention obliges signatory states to take legislative and other measures to effectively address and penalize such crimes.

Furthermore, the Convention facilitates international cooperation and mutual assistance in the investigation and prosecution of cybercrimes, including those that disproportionately affect children, such as online grooming, cyberbullying, and the distribution of child exploitation material.¹⁷⁶ The mechanisms for information sharing, extradition, and joint investigations play a crucial role in tracking down perpetrators who exploit children online, transcending borders in a way that reflects the global nature of the internet.

The Convention's emphasis on capacity building and the exchange of information among parties also supports the development of strategies and technologies to protect children online.¹⁷⁷ By fostering a culture of collaboration, the Convention encourages the sharing of best practices and legal frameworks that can be domestically adapted to enhance children's online safety.

While the Budapest Convention primarily targets the broader challenge of cybercrime, its indirect impacts on children's online safety are significant. It creates a legal and cooperative framework that enables countries to better protect children from online exploitation and abuse. However, the dynamic and evolving nature of cyber threats necessitates continuous updates and adaptations of the legal frameworks.

172. Council of Europe, Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185, <https://rm.coe.int/1680081561>.

173. *Id.*

174. *Id.*

175. *Id.* at 6–7.

176. *Id.* at 14–15.

177. *Id.* at 20–21.

V. BALANCING PARENTAL RIGHTS AND CHILDREN'S DIGITAL PRIVACY RIGHTS

The practice of sharenting has brought to the forefront a complex and intricate balance that must be struck between parents' right to direct the upbringing of their child and the child's digital right to privacy. As social media and digital platforms continue to permeate every aspect of people's lives, parents have unprecedented opportunities to share their children's experiences and milestones with a vast online audience. However, the question of whether such sharing is appropriate, ethical, and respectful of the child's privacy has become a matter of intense debate. On the one hand, parents may feel entitled to share their child's life freely as they deem fit, while on the other hand, children are entitled to a sense of privacy and agency over their digital footprint. The delicate balance between these competing interests must be carefully considered, as any misstep may result in harm to the child's privacy or sense of autonomy. Therefore, it is crucial to navigate the complex terrain of sharenting with sensitivity, respect, and an appreciation of the child's rights and interests, while still enabling parents to celebrate and share their child's growth and development with their network.

Barbara Bennett Woodhouse suggests that parents ought to act like stewards rather than owners concerning their kids¹⁷⁸ because children have the right to be free from their parents' public disclosures.¹⁷⁹ Scholars Benjamin Shmueli and Ayelet Blecher-Prigat agree with Bennett Woodhouse and add that children should have a right to privacy independent from their parents.¹⁸⁰

Erin O'Neill proposes a different approach whereby parents making money off of their children online should be required to follow state work-permit laws that have been implemented to protect child performers, as well as Coogan laws¹⁸¹ for the management of trust accounts.¹⁸²

Katie Hamming posits that Congress should adopt a tort-based approach that aims to narrowly limit a parent's disclosure of their children's PII online, which would allow for a private right of civil action

178. Barbara Bennett Woodhouse, *Hatching the Egg: A Child-Centered Perspective on Parent's Rights*, 14 CARDOZO L. REV. 1747, 1755 (1993).

179. Steinberg, *supra* note 24, at 861.

180. Shmueli & Blecher-Prigat, *supra* note 39.

181. The Coogan Act or the California Child Actor's Bill is a law in California that aims to protect child entertainers by requiring a portion of their earnings to be set aside in a trust fund that is inaccessible until they reach the age of majority. *See* Coogan Act, ch. 637, § 1, 1939 Cal. Stat. 2064, 2064-65 (1939).

182. Erin E. O'Neill, *Influencing the Future: Compensating Children in the Age of Social-Media Influencer Marketing*, 72 STAN. L. REV. ONLINE 42, 44 (2019), <https://www.stanfordlawreview.org/online/influencing-the-future/> [<https://perma.cc/LFD4-3UAD>].

by the child—aged sixteen or older—if actual harm occurred as a result of sharenting.¹⁸³

Amanda Riggio points out that social media platforms can modify their guidelines to protect children.¹⁸⁴ Although Riggio focuses on child entertainers in her analysis, her conclusion is easily adaptable in the context of sharenting. Social media platforms need to self-regulate to include additional guidelines for users uploading content involving minors.¹⁸⁵

Dean Leah A. Plunkett believes that the right to privacy should be protected by a federal statute. She explains that shared content is being exploited “via channels of interstate commerce such as the Internet,” and that the commerce clause grants Congress broad powers to regulate interstate commerce.¹⁸⁶ Plunkett proposes the Protecting the Private Lives of Adolescents and Youth Act (PPLAY). This proposed federal law prohibits “technology companies from using all private digital data collected from any source about children under eighteen for targeted advertising or marketing, as well as decision-making about major life opportunities.”¹⁸⁷ Under PPLAY, PII collected about a child will remain protected after the child in question turns eighteen.¹⁸⁸

However, legislation is not the only solution. Professor Steinberg explains that small routine changes can help parents protect their children’s privacy when engaging in sharenting.¹⁸⁹ Parents should familiarize themselves with the privacy policies of the websites they use to share information and consider sharing anonymously at times.¹⁹⁰ They should be cautious about sharing their child’s actual location, and avoid posting pictures that show their children in any state of undress.¹⁹¹ Giving their child “veto power” over online disclosure, including images and PII, can also help to protect their privacy at a certain age.¹⁹² Finally, parents should be mindful of the potential impact that sharing can have on their child’s current and future sense of self and well-being.¹⁹³

In the digital era, where the boundaries between public and private life increasingly blur, establishing a global standard on privacy emerges as a

183. Kate Hamming, *A Dangerous Inheritance: A Child’s Digital Privacy*, 43 SEATTLE U. L. REV. 1033, 1040, 1056 (2020).

184. Amanda G. Riggio, *The Small-er Screen: YouTube Vlogging and the Unequipped Child Entertainment Labor Laws*, 44 SEATTLE U. L. REV. 493, 522 (2021).

185. *Id.* at 525.

186. PLUNKETT, *supra* note 29, at 481; U.S. Const. art. I, § 8, cl. 3.

187. PLUNKETT, *supra* note 29, at 481.

188. *Id.*

189. Steinberg, *supra* note 24, at 882.

190. *Id.*

191. *Id.* at 880.

192. *Id.* at 881.

193. *Id.* at 882.

critical necessity to safeguard the intrinsic rights of individuals, particularly vulnerable populations such as children. The phenomenon of sharenting underscores the urgent need for a cohesive and universally applicable framework that respects and protects the privacy of the youngest members of our society. This Article advocates for the formulation and adoption of a global standard on privacy, one that is designed to shield every human being's privacy right, with a special emphasis on children, thereby ensuring that as children transition into adulthood, they retain autonomy over their digital footprint.

Such a standard would not only harmonize privacy laws across jurisdictions but also set forth clear guidelines for digital conduct respecting children's rights. It would delineate the boundaries of acceptable sharing, firmly grounding parents' actions within a framework that prioritizes the child's long-term welfare and consent. This global privacy standard would require the cooperation of international bodies, governments, civil society, and technology companies to create a protective net around the digital lives of children. It would encompass robust provisions for consent, specifically tailored for the digital age, where a child's understanding and capacity evolve with age, ensuring that the right to privacy is both a proactive and reactive safeguard against unwanted digital exposure.

The proposed standard would also address the commercial exploitation of children's data, drawing from principles similar to those proposed in PPLAY, but extending its reach globally. It would mandate technology companies to adopt stringent measures in handling data related to minors, prohibiting the use of such data for targeted advertising or decision-making that could impact a child's future opportunities. Furthermore, this standard would advocate for digital erasure rights, allowing individuals to have control over their digital past, ensuring that information shared during childhood does not unduly influence their future.

CONCLUSION

In the brick-and-mortar era, parents announcing to the world that their children had reached a specific milestone, such as walking on both feet or riding a two-wheeler by placing advertisements in the local paper was not a commonly accepted practice. Yet, in the age of social media, sharenting has become an increasingly common practice among parents seeking to share their joy and connect with their loved ones.¹⁹⁴ However, while sharing images and information about one's children can have positive social benefits, it is important to acknowledge the potential risks and negative consequences that can arise from this practice. One of the

194. See discussion *supra* Section I.A.

most concerning risks is the possibility of images or videos of children falling into the hands of predators who may use them for nefarious purposes.¹⁹⁵ Furthermore, the ease with which digital images can be manipulated and altered means that even innocuous images can be morphed into something harmful and make their way onto the dark web, posing a serious threat to children's safety and privacy.¹⁹⁶

Moreover, the legal frameworks in the United States and across the world have not kept pace with the rapid changes in technology.¹⁹⁷ As such, there is a pressing need to strike a balance between a parent's right to direct the upbringing of their child and a child's right to privacy.¹⁹⁸ To achieve this balance, it is essential to promote greater awareness among parents of the potential risks of sharenting online, as well as the importance of implementing stricter privacy settings while sharing on social media platforms, which can help safeguard children's privacy and protect them from malicious actors.¹⁹⁹ In addition, the universal nature of digital technology and its impact on children's rights necessitate a global approach. A global privacy standard would not only offer a coherent strategy for protecting children in the digital space but also affirm the global community's commitment to upholding the dignity, autonomy, and privacy of every individual, laying a foundation for a future where digital empowerment does not come at the cost of personal privacy.²⁰⁰

195. See discussion *supra* Section I.B.

196. See discussion *supra* Section II.C.

197. See discussion *supra* Sections III.B, IV.

198. See discussion *supra* Section V.

199. *Id.*

200. *Id.*