A Dangerous Inheritance: A Child's Digital Identity

*Kate Hamming**

"[Y]ou can choose your friends but you sho' can't choose your family, an' they're still kin to you no matter whether you acknowledge 'em or not, and it makes you look right silly when you don't."[1]

ABSTRACT

This Comment begins with one family's story of its experience with social media that many others can relate to in today's ever-growing world of technology and the Internet. Technology has made it possible for a person's online presence to grow exponentially through continuous sharing by other Internet users. This ability to communicate and share information amongst family, friends, and strangers all over the world, while beneficial in some regard, comes with its privacy downfalls. The risks to privacy are elevated when children's information is being revealed, which often stems from a child's own parents conduct online. Parents all over the world are creating their children's digital identities before these children even have the chance to develop them on their own. And other safety issues are often overlooked, such as those relating to online pedophiles and identity theft. This Comment argues the need for a legislative solution in the United States incentivizing adults to restrict the types of information that they choose to disclose online. However, such legislation must consider First Amendment hurdles and incorporate realistic and unambiguous restrictions, which are based in tort law and provide for a private right of action that can ultimately serve the specific

* J.D. Candidate 2020, Seattle University School of Law; B.A., University of Washington; Symposium Chair, Seattle University Law Review. I would like to thank Trisha Gum and Sasha Zimonjic of Film and Ink Law Group for encouraging me to tackle an article topic based in privacy law and the Internet of things. I also wish to give a special thanks to Ian for supporting me throughout my law school career and all of the long and tiresome nights spent reading and writing that came along with the journey.

1. HARPER LEE, TO KILL A MOCKINGBIRD 84 (1960).

purpose of protecting children's privacy until reaching an age when they can do so themselves.

CONTENTS

INTRODUCTION

Roman Dinkel, now aged two, was diagnosed with spina bifida[2] when his mother was twenty weeks pregnant.[3] While in utero, Roman underwent surgery to improve the breathing and functional-movement issues that he would struggle with after he was born.[4] Before his birth, doctors told his parents there was a chance that Roman would not be able to walk.[5] However, with the help of physical therapy, he began using a walker a year after he was born.[6] At the age of two, he was able to use crutches on his own to take his first independent steps.[7]

In an effort to shed light on spina bifida, Roman's parents created a Facebook page to share updates regarding his diagnosis, "Defying Odds: Roman's Journey,"[8] which has almost 400,000 followers.[9] After Roman's parents shared a video of him celebrating his first steps, the post "went

2. "Spina bifida is a condition that affects the spine and is usually apparent at birth. . . . Spina bifida might cause physical and intellectual disabilities that range from mild to severe." *What Is Spina Bifida?*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/ncbddd/spinabifida/facts.html [https://perma.cc/XY6J-3R4K].

3. Nicole Pelletiere, *Toddler with Spina Bifida Warms Hearts After Showing His Dog He Can Walk*, GOOD MORNING AM. (Aug. 10, 2018), https://www.goodmorningamerica.com/family/story/toddler-spina-bifida-warms-hearts-showing-dog-walk-57132496 [https://perma.cc/2TB3-HZPY].

4. *Id.*

5. *Id.*

6. *Id.*

7. *Id.*

8. *Id.*

9. Adam Dinkel, *Defying Odds: Roman's Journey*, FACEBOOK, https://www.facebook.com/romanclevelanddinkel/ [https://perma.cc/V9FC-BZHG].

viral"[10] garnering the attention of Good Morning America (GMA).[11] The broadcast-television show reposted the video on the GMA Facebook page, in turn capturing over 99 million views.[12]

Roman's videos receive comments from millions of people who express joy in witnessing Roman's adventures, and many have expressed that his videos have "improved their moods and changed their lives for the better."[13] In fact, surveys of patients and their families have shown that many people join similar online groups and pages to seek support, provide support for others, and educate themselves.[14] Similarly, reports show that nearly seventy-five percent of parents using social media do so for purposes of seeking parenting-related information, advice, and support.[15] While these videos may have the capability to inspire and support millions of strangers, Roman's parents have exploited intimate details in exchange for those intangible benefits before he has even reached an age where he can voice his opinion on the matter.

Many viewers may passively watch these videos and simply move on with their lives, but a risk to Roman's safety may also exist when considering the potential number of ill-intentioned viewers, such as child predators or stalkers.[16] In fact, investigations into pedophile image-sharing sites have shown that over 20 million images were directly sourced from social media.[17] Further, other often unrecognized harms result from sharing psychosocial or embarrassing information that could be misused

---

10. When something online goes viral, it has "spiked in popularity" among a large number of viewers and users over a short amount of time. *Viral*, TECHTERMS (Feb. 9, 2011), https://techterms.com/definition/viral [https://perma.cc/3R4T-ZTFS].

11. Pelletiere, *supra* note 3.

12. *Id.*

13. *Id.*

14. Robyn Jacobs et al., *The Importance of Social Media for Patients and Families Affected by Congenital Anomalies: A Facebook Cross-Sectional Analysis and User Survey*, 51 J. PEDIATRIC SURGERY 1766 (2016).

15. Meave Duggan et al., *Parents and Social Media*, PEW RES. CTR. (July 16, 2015), https://www.pewresearch.org/internet/2015/07/16/parents-and-social-media/ [https://perma.cc/SP4P-ZQZ3].

16. *See* Winhkong Hua, Note, *Cybermobs, Civil Conspiracy, and Tort Liability*, 44 FORDHAM URB. L.J. 1217, 1223 (2017) (addressing the correlation between the growth of Internet usage and usage of the Internet as a medium for bad behavior).

17. Lucy Battersby, *Millions of Social Media Photos Found on Child Exploitation Sharing Sites*, SYDNEY MORNING HERALD (Sept. 30, 2015), https://www.smh.com.au/national/millions-of-social-media-photos-found-on-child-exploitation-sharing-sites-20150929-gjxe55.html [https://perma.cc/P72Q-FPL4] (discussing a certain child-exploitation site with over 45 million images); *see also* Raymond Lengel, *Psychosocial Assessment: A Nursing Perspective*, CEUFAST (Mar. 10, 2017), https://ceufast.com/course/psychosocial-assessment-a-nursing-perspective [https://perma.cc/NLQ6-JDUJ] (defining psychosocial information as information pertaining to a person's mental health or social well-being).

by viewers, and even identity theft can occur.[18] All parents should consider a number of risks before exposing such intimate details as their children's full names, photographs, and health information.

The family setting embodies a sacred cultural and legal institution historically protected from societal and governmental interference.[19] Communitarian theorists argue that any law focusing on the individual interests of family members is inappropriate for this setting and could harm the sense of collective and loving relationships, which are a fundamental part of every household.[20] Specifically, this ideology mirrors the general public's desire to avoid laws that interfere with parents' general right to autonomously make decisions regarding their children, unless the children are old enough to have a say in important decisions that personally affect their lives.[21] But what about important decisions that personally affect a child's life but are made before a child is old enough provide consent or take control? Parents make innumerable decisions before their children are old enough to provide meaningful approval, such as imposing certain dietary restrictions, picking a private school over a public school, or forcing certain recreational activities upon a child. However, parents are increasingly making one choice that may pose greater long-term harm to their children: "sharenting" of sensitive personal information.[22]

Sharenting refers to parental disclosures through online posting of pictures and information about all aspects of their children's lives.[23] While it is rare that parents share with malicious intentions, many parents do not consider the potential reach and long-term consequences of sharing sensitive personal information about their children on highly public

18. *See generally* Bahareh E. 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 (2017).

19. *See* Martha Albertson Fineman, *Our Sacred Institution: The Ideal of the Family in American Law and Society*, 1993 UTAH L. REV. 387, 388 (1993); *U.S. Supreme Court Limits Government Ability to Interfere with Parents' Child-Rearing Decisions*, AM. CIV. LIBERTIES UNION (June 5, 2000), https://www.aclu.org/news/us-supreme-court-limits-government-ability-interfere-parents-child-rearing-decisions [https://perma.cc/6MG8-UR7A] [hereinafter *SCOTUS Limits*].

20. Benjamin Shmueli & Ayelet Blecher-Prigat, *Privacy for Children*, 42 COLUM. HUM. RTS. L. REV. 759, 774–75 (2011).

21. *SCOTUS Limits*, *supra* note 19; *see also* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501(1), 6502(a)–(b)(2) (2019) (defining a child as someone under the age of thirteen and providing that parental consent is no longer required after the age of thirteen).

22. *See* Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 EMORY L.J. 839, 843 (2017); Duggan et al., *supra* note 15 (reporting that ninety-four percent of parents using Facebook share or post to the site instead of using it simply to read or view content).

23. Nione Meakin, *The Pros and Cons of 'Sharenting,'* GUARDIAN (May 18, 2013), https://www.theguardian.com/lifeandstyle/2013/may/18/pros-cons-of-sharenting [https://perma.cc/6K3H-ENHU].

forums.[24] Information on the Internet is forever, and a child's past and behavior can be googled[25] if such information was previously exposed online—by anyone, anytime.[26] Further, sharenting impedes children's ability to create their own digital identities and their overall right to privacy.[27] Sharenting can thus impact children psychosocially[28] or result in identity theft or exposure to online predators.[29]

United States (U.S.) society, including policymakers and legislators, must do more to protect privacy relating to children's sensitive personal information. Broadly, the sensitive personal information needing protection should include the type of information that could be used to inflict privacy or security harm if placed into "the wrong hands": the type of information that imposes "a risk of harm resulting from a loss of control over information."[30] Lawmakers increasingly recognize the need for a subcategory of personal information subject to higher risks by including separate provisions addressing its heightened protection, including provisions protecting one's racial or ethnic origin, biometric data, sexual orientation, among a myriad of other information. For example, the European Union's (EU) General Data Protection Regulation (GDPR), enacted in May 2018, includes provisions regarding the processing of sensitive personal information.[31] The GDPR's global influence reflects the growing privacy concern associated with personal information data in the

---

24. Adrienne LaFrance, *The Perils of 'Sharenting,'* ATLANTIC: TECH. (Oct. 6, 2016), https://www.theatlantic.com/amp/article/502757/ [https://perma.cc/67TL-M6QK].

25. To "google" means "to use the Google search engine to obtain information about (someone or something) on the World Wide Web." *Google*, MERRIAM WEBSTER (11th ed. 2019).

26. Mollie Brunworth, *How Women Are Ruining Their Reputations Online: Privacy in the Internet Age*, 5 CHARLESTON L. REV. 581, 602 (2011).

27. Steinberg, *supra* note 22, at 842.

28. Ego psychologist Erik Erickson developed the theory of psychosocial development, which asserts that individuals develop their personalities in a series of eight stages: "Each stage in Erikson's theory builds on the preceding stages and paves the way for the following periods of development." Kendra Cherry, *Erik Erikson's Stages of Psychosocial Development*, VERYWELL MIND (Jan. 4, 2019), https://www.verywellmind.com/erik-eriksons-stages-of-psychosocial-development-2795740 [https://perma.cc/5NY7-78JT]. This theory is one of the most widely accepted and influential theories of personality development. *Id.*

29. Jacqueline Howard, *The Dos and Don'ts of Posting About Your Kid Online*, CNN: HEALTH (Oct. 21, 2016), https://www.cnn.com/2016/10/21/health/posting-about-kids-on-social-media/index.html [https://perma.cc/6CC5-MU34].

30. Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1133 (2015).

31. Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 9, 2016 O.J. (L 119) 38 (EU) [hereinafter GDPR] (categorizing sensitive information as "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership . . . genetic data, biometric data [processed] for the purpose of uniquely identifying a . . . person . . . health [data] or data concerning a . . . person's sex life or sexual orientation").

modern world that continues to be subject to consistent technological innovation and advancement.

Therefore, a legislative need demands that laws expressly call out children's information as an additional subcategory of personal information that is similarly vulnerable to higher risks and deserving of heightened protection. The potential harm to children's right to privacy and ability to form their own online identities increases exponentially and proportionately with the number of viewers of their information. Therefore, public figures, such as celebrities, exemplify the problem because, when they post pictures of and information about their children on their public social media accounts, the potential reach of that information spikes in breadth because people around the world actively follow celebrities' lives. For instance, Kylie Jenner, a reality television star with over 100 million Instagram followers, received over eighteen million "likes" and almost two million comments on the first picture she posted of her daughter, Stormi.[32] As her daughter ages, Jenner continues to share more and more photographs and videos revealing her daughter's face and voice to over 130 million strangers.[33] Children cannot choose whether or not they are born to famous parents, but they should be able to choose whether or not to publicly expose certain private aspects of their life, just as their parents can. Moreover, as exemplified by Roman Dinkel's situation, average civilians can achieve public-figure status, as measured by the number of followers and views, when their posts go viral.

This Comment is the first to argue that the best solution lies in the enactment of federal legislation incentivizing self-censorship in parental disclosures of a child's sensitive information on social media, or similar interactive websites, by providing a private cause of action for a child who suffers from a cognizable injury. This legislation should be grounded in the invasion of privacy and encompass provisions modeled after the tort of Publicity Given to Private Life.[34] Moreover, the proposed law should specifically contemplate parents who have public-figure status, a term defined therein, because such persons are inherently put on notice of the risks stemming from the ease of accessibility and exposure to their information.

Part I provides a brief history of advancing technology's effects on privacy concerns relating to personal information. It will discuss recent legislative and regulatory emphasis on the special category of "sensitive

32. Lori Keong & Rachel Epstein, *The Top 10 Most-Followed Celebrities on Instagram in 2018*, MARIE CLAIRE (Feb. 21, 2018), https://www.marieclaire.com/celebrity/a23863/most-followed-celebrities-on-instagram-in-2016/ [https://perma.cc/CHN5-ZVBT].

33. *See* Kylie Jenner (@kyliejenner), INSTAGRAM, https://www.instagram.com/kyliejenner/?modal=true&hl=en [https://perma.cc/9QKA-WHHK].

34. RESTATEMENT (SECOND) OF TORTS § 652D (1977).

personal information" and analyze recent U.S. Supreme Court decisions on the issue. Additionally, Part I will outline new dangers associated with sensitive personal information specifically resulting from advances in biometrics. Part II explores sharenting and the potential danger in parental disclosures of children's sensitive personal information. Part III explores children's privacy rights around the world and how relevant issues are approached in other countries; it will compare these international perspectives to the current state of the United States' child-privacy rights. Part IV will acknowledge and respond to potential First Amendment challenges asserting a parent's right to freedom of speech, ultimately concluding that the government's interest in protecting a child's privacy should outweigh any First Amendment challenge. Lastly, Part V argues for domestic federal legislation under a tort theory that contains some aspects of current policies and solutions. Part V concludes by discussing why the solution should prescribe children the right to a cause of action against their parents rather than the technological entities.

I. ADVANCING TECHNOLOGIES AND DECLINING PRIVACY

People inherently value their privacy and, therefore, they value having control over who knows what about their personal life.[35] These values increasingly come into conflict as a result of advances in information technology that both reduce the amount of such control and open the door to negative consequences resulting from unwanted access to personal data.[36] The increasing power and capabilities of new technology, coupled with the sentiment of declining clarity and agreement regarding what constitutes personal information privacy, have continued to pose legal challenges.[37] Furthermore, these combatting forces have recently influenced government entities to propose and enact new legislation.[38]

Most notably, the European Union (EU) made progress with its enactment of the GDPR, which provides a new and expansive regulatory framework for consumer data protection and took effect in May 2018.[39] The regulation is viewed as one of the "most robust data privacy laws in the world" and sets new and higher standards for data processing among

35. JEROEN VAN DEN HOVEN ET AL., *Privacy and Information Technology, in* STANFORD ENCYCLOPEDIA OF PHILOSOPHY 1 (2019), https://leibniz.stanford.edu/friends/preview/it-privacy/ [https://perma.cc/ZG5A-EYSN].

36. *Id.*

37. *Id.*

38. *See* GDPR, *supra* note 31, at 1–2; California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.175 (West 2018) (effective Jan. 1, 2020) [hereinafter CCPA].

39. Arielle Pardes, *What Is GDPR and Why Should You Care?*, WIRED: GEAR (May 24, 2018), https://www.wired.com/story/how-gdpr-affects-you/ [https://perma.cc/76SC-9HN9].

all companies that target "data subjects" that are EU citizens.[40] The GDPR represents a privacy revolution that is changing the way companies handle consumer privacy and provides people with new rights to control their personal information on the Internet—with its effects reaching far beyond Europe's borders.[41]

Recently, in efforts to legislate privacy, various jurisdictions have attempted to define "personal data." The GDPR defines personal data as "information relating to an identified or identifiable natural person."[42] Similarly, the California Consumer Privacy Act of 2018 (CCPA) defines personal information as "information that identifies . . . a particular consumer or household."[43] Privacy-related legislation or regulation universally tends to define personal information by its ability to identify a person; the term "personally identifiable information" (PII) is often used when referring to the type of information that privacy laws aim to protect.[44]

However, PII is a term that covers a broad spectrum of information that can be used to identify someone, so many lawmakers have begun to recognize a subcategory of PII: sensitive personal information. For instance, GDPR recognizes that certain types of sensitive information[45] warrant "specific protection" and prohibits the processing of this kind of information, unless any of its listed exceptions are met.[46] The GDPR justifies the need for heightened protection because that type of information "could create significant risks to . . . fundamental rights and freedoms."[47] This type of information is viewed as information that could lead to material contractual or legal liability, damage to one's image or reputation, or financial losses if disclosed to or used by someone with wrongful intentions.[48]

The GDPR's acknowledgment of a separate category of sensitive information echoes society's heightened expectation of privacy that continues to grow alongside advancing technology.[49] Examples of the

40. *Id.*

41. *See Id.*

42. GDPR, *supra* note 31, at 33 (art. 4(1)).

43. CCPA, CAL. CIV. CODE § 1798.140(o)(1) (West 2018).

44. *See* 2 C.F.R. § 200.79 (2013).

45. *See supra* text accompanying note 31.

46. GDPR, *supra* note 31, at 38 (art. 9), 33 (art. 4) (defining "processing" as any operation performed on personal data, including "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction . . . .").

47. GDPR, *supra* note 31, recital 51.

48. Ohm, *supra* note 30.

49. ROBERT BRAUNEIS & ROGER E. SCHECHTER, COPYRIGHT: A CONTEMPORARY APPROACH 1 (2d ed. 2018).

types of sensitive information that people expect to remain private include cell phone location and biometric data. A recent U.S. Supreme Court case, *Carpenter v. United States*, reflected this view and held that the sensitive information on a cell phone benefits from a reasonable expectation of privacy—meaning the Court may start taking a more extensive view on privacy.[50] The Court reasoned that because historical cell-site records provide an "intimate window" into the user's "'familial, political, professional, religious, and sexual associations,'" location records deserve heightened protection—namely, the Constitution demands a search warrant before the government can search or seize such information.[51] The Court attributed technology to enhancing the general capacity to intrude upon areas typically protected from "inquisitive eyes."[52] While the Court narrowly decided the case in the context of law enforcement requests for location information, the Court's decision suggests that the Supreme Court is likely to continue the trend by taking a broader view on reasonable privacy expectations in the digital era.[53]

In addition to data derived from location technology, advances in biometrics involve dangers associated with sensitive personal information in today's tech savvy world.[54] Included in the GDPR's category of sensitive personal information,[55] biometrics is the "[a]utomated recognition of individuals based on their biological and behavioural characteristics."[56] Biometric technology uses a person's unique identifiable features, such as a fingerprint or face, to validate the person's identity.[57] These technologies, which are used for both online verification purposes[58] as well as marketing purposes,[59] present separate dangers for online participants and consumers.

---

50. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

51. *Id.* at 2217.

52. *Id.* at 2214.

53. J.G. Harrington, Carpenter v. United States*: What It Means for Companies That Collect Location Data*, COOLEY (June 28, 2018), https://www.cooley.com/news/insight/2018/2018-06-28-carpenter-v-united-states-what-it-means-for-companies-that-collect-location-data [https://perma.cc/6R5D-UBPE].

54. *See generally* DEP'T OF TREASURY, THE USE OF TECHNOLOGY TO COMBAT IDENTITY THEFT (2005), https://www.hsdl.org/?view&did=482322 [https://perma.cc/HH5W-EELC].

55. GDPR, *supra* note 31, at 38 (art. 9(1)).

56. *Biometrics Definition*, BIOMETRICS INSTITUTE: WHAT IS BIOMETRICS?, https://www.biometricsinstitute.org/what-is-biometrics/ [https://perma.cc/TY9H-GGTF].

57. *Id.*

58. *New Trends in Biometrics [March 2018] with Isabelle Moeller from the Biometrics Institute*, GEMALTO: CASE STUDIES (June 3, 2018), https://www.gemalto.com/govt/biometrics/trends-in-biometrics [https://perma.cc/UVJ3-VRJ8] [hereinafter *New Trends*].

59. Anne T. McKenna, *Pass Parallel Privacy Standards of Privacy Perishes*, 65 RUTGERS L. REV. 1041, 1065 (2013).

First, in the online verification context, more institutions are beginning to use biometric technology to provide stronger identity verification measures for people trying to access computers, airlines, and other typically restricted areas.[60] For example, the North American Free Trade Agreement (NAFTA) reported that banks have been instructed to utilize facial and voice recognition technology to verify online identification.[61] Such technology should be viewed as a double-edged sword: on one hand, it has the ability to fight fraud by providing people with a convincing proof of identity[62] if the sensitive personal information inherent to the technology's use remains protected; on the other hand, it has the juxtaposing ability to provide an avenue for identity theft and fraud if the information is made accessible to those aiming to commit wrongdoing. Experts in the field advise against using biometric technology as a single-factor authentication method for this reason and instead promote the integration of biometric technology into already existing verification processes to provide for a stronger multi-factor authentication solution.[63]

Second, technologies exist that are capable of storing biometric information for marketing purposes, such as a user's facial or voice biometrics.[64] The perpetual storage of sensitive personal information creates the risk that such information will be subject to irresponsible or inappropriate use,[65] such as a marketer tracking a child's location in public places by using the child's facial biometrics, which were obtained from a social media site that scanned and recorded the information.[66] This tracking could result in the gathering of data that essentially equates to geolocation information, which is classified as sensitive personal information due to its revealing nature—especially when considering the special privacy interest associated with the safety of a child.[67] A few state laws exist, like Texas, that aim to combat the inappropriate use of biometric information obtained for marketing purposes by imposing requirements to inform the person and gain the person's consent before capturing such information for commercial purposes.[68] However, these

60. *Biometrics Definition*, *supra* note 56.

61. *New Trends*, *supra* note 58.

62. *Id.*

63. *Id.*

64. Carmen Aguado, Comment, *Facebook or Face Bank?,* 32 LOY. L.A. ENT. L. REV. 187, 192–93 (2012).

65. *See* Maria Korolov, *What Is Biometrics? And Why Collecting Biometric Data Is Risky*, CSO (Feb. 12, 2019), https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html [https://perma.cc/AD5D-7CHR].

66. McKenna, *supra* note 59.

67. Ohm, *supra* note 30, at 1180.

68. *See* TEX. BUS. & COM. CODE ANN. § 503.001(b) (West 2017).

laws merely prescribe a maximum fine per violation and lack a private right of action for consumers, which privacy attorneys believe could have deterred companies from participating in inappropriate capturing.[69] Therefore, stronger protection from these newer harms and potential redress for children still remains absent from privacy legislation in the United States.

II. SHARENTING AND ITS ADVERSE IMPACT ON CHILD DEVELOPMENT

A new norm of oversharing information continues to grow in conjunction with the emergence of new technologies. Celebrities previously known for shying away from the paparazzi are modeling this new norm and choosing to share photographs and information on social media, arguably reaching far more viewers than magazines or entertainment television ever has, and they are able to do so in real time—such as using Facebook or Instagram Live. Perhaps it is because technology now allows them to control what information is exposed and many celebrities use social media platforms as viable tools for self-promotion.[70] However, as seen in the case of the Dinkel family, the viral nature of today's Internet provides ways for the average citizen to achieve a celebrity status that would have been unachievable before the boom of the digital age.[71] With this heightened status comes the heightened risk to privacy associated with oversharing of personal information because the likelihood that the information will get into the wrong hands increases exponentially. As privacy risks heighten, so does the need to protect children's information from the potential breadth of exposure resulting from the unique nature of today's online world.

Technology and the Internet present new issues that need non-traditional solutions because "networked publics have different characteristics than traditional physical public spaces."[72] The four unique characteristics of online public spaces that create new challenges to privacy are (1) persistence (the durability of online expressions and information), (2) visibility (information's potential audience), (3)

---

69. Paul Shukovsky, *Washington Biometric Privacy Law Lacks Teeth of Illinois Cousin*, BLOOMBERG L.: PRIVACY & DATA SEC'Y (July 18, 2017), https://www.bna.com/washington-biometric-privacy-n73014461920/ [https://perma.cc/EWX8-ESN9].

70. *See generally* Kelsey Skager, *How Celebs Use Social Media for Self-Promotion and Charity*, QUALITY LOGO PRODUCTS BLOG: MARKETING & BRANDING (Apr. 4, 2012), https://www.qualitylogoproducts.com/blog/celebrity-social-media-self-promotion-charity/ [https://perma.cc/658G-DQNM].

71. *See generally* Todd Leopold, *Privacy? Forget It, We're All Celebrities Online Now*, CNN: BUS. (June 12, 2013), https://www.cnn.com/2013/06/12/tech/social-media/internet-privacy-divide/index.html [https://perma.cc/GH68-GUQT].

72. Danah Boyd, *It's Complicated: The Social Lives of Networked Teens*, *in* INTERNET LAW: CASES & PROBLEMS 143, 143 (9th ed. 2019).

spreadability (the ease with which information is shared), and (4) searchability (the ability to find information).[73] Persistence means that information shared does not expire once viewed or read by another, and it could be kept or exist for decades. Visibility means that what is shared online is more widely accessible across far and unknown destinations "because most systems are designed such that sharing with broader or more public audiences is [the] default," which is different than people needing to make concerted efforts to expose information to larger audiences when in a physical space.[74] Spreadability is the greatest difference for Internet spaces because the technology allows people to spread information, whether by intentionally or indirectly encouraging sharing "with the click of a few keystrokes," in ways that can be easily downloaded or forwarded to others.[75] Lastly, searchability is another trait of the online world that raises cause for concern because strangers and people from all over the world can search databases to uncover countless types of information shared by or about others.[76]

Consequently, these characteristics distinguish the Internet space from the physical space by amplifying social situations. As technology advances and develops, people use the technical features and "help create new social dynamics."[77] One of the new social dynamics underlying the concern for children's online privacy occurs when people "stalk" others "by searching for highly visible, persistent data" about a certain person of interest.[78] Eventually, such stalking can lead to exploiting information about someone in a way that adversely affects the person's life by taking advantage of the spreadability of the Internet.[79] Hence, Internet-users need to consider carefully the information they choose to share online because the extent and degree of potential problems may never be reversible. Taking such care is especially important when parents share content online revealing intimate information about their children.

A distinct type of oversharing by parents has been referred to as "sharenting," which describes the growing trend among parents to share information about their children on the Internet.[80] Parents have a number

73. *Id.*
74. *Id.* at 143–44.
75. *Id.* at 144.
76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.*
80. Steinberg, *supra* note 22, at 842. *See generally* TEHILA MINKUS ET AL., CHILDREN SEEN BUT NOT HEARD: WHEN PARENTS COMPROMISE CHILDREN'S ONLINE PRIVACY (2015), http://cse.poly.edu/~tehila/pubs/WWW2015children.pdf [https://perma.cc/X9GW-YX6A] (acknowledging Facebook and Instagram as two of the major platforms and reporting that the number of parents who post pictures of their children falls in the range of 66–98%).

of reasons why they choose to discuss their children's details online, ranging from fulfilling the desire to stay connected with family and friends to attempting to feel less alone when experiencing the hardships and challenges of parenting.[81] Although these reasons are seemingly innocent, these parents are placing their interests in sharing above the more compelling interests of their children when they choose not to consider the associated risks. While it is true that oversharing personal information, regardless of one's age, could lead to risky exposure impacting one's privacy,[82] American society should recognize the heightened interest in protecting children's personal information.

Further, sharenting leads to two different types of privacy issues: (1) general child safety or security and (2) psychosocial development.[83] First, the danger to a child's safety resulting from online parental sharing is best exemplified by a mother's frightening true story. A mother, who was an online-blogger,[84] learned her lesson after posting photographs of her twins while potty-training them.[85] To her horror, she later discovered that viewers viewed the photos, downloaded and altered the photos, and eventually posted them on a different website that pedophiles often visited.[86] This scenario is a clear example of when a child's interest in privacy should outweigh a parent's interest in feeling connected with the online community, which is a policy the blogger-mother agreed with.[87] Moreover, fifty percent of images on pedophile sites originate from parents' social media postings.[88] Emphasis should be placed on the child's right to safety when considering issues related to child privacy rights versus parental rights to share their lives online.

Second, in addition to the dangers that affect child safety, a parent's oversharing of personal information online can inhibit psychosocial

---

81. Howard, *supra* note 29.

82. *See generally Protect Against Identity Theft When Sharing Photos Online*, EQUIFAX, https://www.equifax.co.uk/resources/identity_protection/protect-against-identity-theft-when-sharing-photos-online.html [https://perma.cc/F2R2-UDW5].

83. Howard, *supra* note 29; *see also* Emily Blatchford, *Should You Post Photos of Your Child on Social Media?*, HUFFINGTON POST AU (Aug. 30, 2017), https://www.huffingtonpost.com.au/2017/08/29/should-you-post-photos-of-your-child-on-social-media_a_23190070/ [https://perma.cc/G5XM-V35R].

84. Bloggers are people, often marketers, who share diverse kinds of information online for readers to view for free. Kipp Bodnar, *29 of the Best Social Media Marketing Blogs of 2018*, HUBSPOT (Sept. 24, 2018), https://blog.hubspot.com/blog/tabid/6307/bid/5977/36-awesome-social-media-blogs-everyone-should-read.aspx [https://perma.cc/63UD-KJVX].

85. Steinberg, *supra* note 22, at 847.

86. *Id.*

87. LaFrance, *supra* note 24.

88. Kristy Goodwin, *Sharenting–What Parents Need to Consider Before Sharing Pictures of Their Kids*, DR. KRISTY GOODWIN (Aug. 22, 2017), https://drkristygoodwin.com/sharenting-what-parents-need-to-consider-before-sharing-pictures-of-their-kids/ [https://perma.cc/P9VT-BVTA].

development through the creation of the child's digital identity.[89] Erik Erikson's phases of psychosocial development outline the eight stages people experience while developing and growing and reflect the impact of certain interactions and relationships.[90] In short, his theory suggests that people experience a conflict at each stage, which serves as a monumental point in development, and "[i]f people successfully deal with the conflict, they emerge from the stage with psychological strengths that will serve them well for the rest of their lives."[91] Notably, stages two and five relate to the issue of a child's digital identity: "Autonomy vs. Shame and Doubt" and "Identity vs. Confusion."[92]

A child's pre-existing online presence may affect the child's successful development in stage two, the Autonomy vs. Shame and Doubt stage. Stage two is the point in development where children should begin to gain independence, and parents can aid by allowing children to gain control through their own choices.[93] The United States is the world leader when it comes to young people's online presence: about ninety-two percent of American children under two-years-old appear in online photographs.[94] Therefore, by the age of two, these children have an online footprint that was created by their parents or other adults and completely out of their control. Erikson believes that "[c]hildren who successfully complete this stage feel secure and confident," while others are left with feelings of self-doubt.[95] People are now expected to participate in the online world,[96] so the act of creating one's online presence should be considered important. Predetermining a child's digital presence through oversharing before the child can make choices autonomously could prevent a successful completion of this point in development, precluding a child from acting "with intention, [and] within reason and limits."[97]

Stage five, Identity vs. Confusion, begins to take place as children submerge into their teenage years and "plays an essential role in developing a sense of personal identity which will continue to influence behavior and development for the rest of a person's life."[98] The inheritance of a digital identity from one's parents could inhibit a child from

89. Howard, *supra* note 29.

90. Cherry, *supra* note 28.

91. *Id.*

92. *Id.*

93. *Id.*

94. Mark Milian, *Study: 82 Percent of Kids Under 2 Have an Online Presence*, CNN (Oct. 7, 2010), http://www.cnn.com/2010/TECH/social.media/10/07/baby.pictures/ [https://perma.cc/UH79-3Q63].

95. Cherry, *supra* note 28.

96. Leopold, *supra* note 71.

97. Cherry, *supra* note 28.

98. *Id.*

independently developing a sense of self because excessive public exposure online can make it very difficult for a child to erase[99] and restart by creating the child's own personal digital identity. This could lead to feelings of insecurity and confusion for the child and the child's future.[100]

On the other hand, research suggests that teens who are able to independently form strong personal identities are more likely to form intimate relationships when they begin to reach adulthood.[101] By the time a child reaches this stage in development, the child's personal identity is typically shaped by the child's experiences with others.[102] However, parents who overshare throughout their child's upbringing can unknowingly shape the opinions and beliefs of others about the child, hindering the chance for the child to mold those experiences with people who already have a sense of the child's identity from what they previously viewed online. In the case of Roman Dinkel, by the time he reaches adolescence, it is likely that both of these stages of development may be impacted by his parents continuous posting—jeopardizing his "intrinsic right to determine his own identity."[103]

While someday Roman may not mind the choices his parents made and the identity they created for him, he should be given the autonomy to choose how he appears to the world and how the world perceives him as an individual. This does not mean that parents should necessarily be restricted from sharing anything about their children online—it just means that more thoughtfulness should go into what types of things they do share. Experts in pediatrics and Internet law recommend that parents should consider how their children will feel someday about pictures of them as babies or teens being posted online, with one expert noting that "children at certain stages do not wish to be photographed or . . . for those photos to be made public."[104] Children may therefore someday resent their parents disclosures made years earlier but may nonetheless be left without remedial measures.[105]

---

99. Milian, *supra* note 94.

100. Cherry, *supra* note 28.

101. *Id.*

102. *Id.*

103. Keith & Steinberg, *supra* note 18, at 413.

104. David Chazan, *French Parents 'Could be Jailed' for Posting Children's Photos Online*, TELEGRAPH (Mar. 1, 2016), https://www.telegraph.co.uk/news/worldnews/europe/france/12179584/French-parents-could-be-jailed-for-posting-childrens-photos-online.html [https://perma.cc/5GPR-CTB4]; *see also* Keith & Steinberg, *supra* note 18, at 413–14.

105. Keith & Steinberg, *supra* note 18.

III. CHILD PRIVACY RIGHTS IN AMERICA VERSUS ABROAD

Currently, no United States federal law exists restricting parents' online activity when it comes to protecting children's personal information privacy nor does any law exist that provides children with a remedy against one's parent.[106] However, legislators have attempted to provide a more general heightened protection for children and their privacy. This section highlights state and federal legislative efforts, with a focus on relevant tort law as well as laws and policies adopted overseas.

Congress enacted the Children's Online Privacy Protection Act in 1998 (COPPA), which requires certain compliance by operators of online services directed at children under the age of thirteen;[107] the Federal Trade Commission (FTC) updated the Act in 2013 to account for changes in technology.[108] Although violations in compliance can result in civil penalties, COPPA specifically applies to entities "that collect personal information from children under thirteen" years old and requires parental consent before personal information is collected from children.[109] Rather, COPPA gives parents the authority to consent to the collection of their children's information and, thus, the ultimate authority to make choices about their children's data privacy.[110]

Congress proposed to amend COPPA with the "Clean Slate for Kids Online Act of 2018,"[111] which provides individuals the opportunity to reconcile unwanted or regretful Internet activity carried out before that individual's thirteenth birthday.[112] This bill only applies to online activity carried out by a child before reaching thirteen years old and gives those individuals the option to delete personal information collected from them prior to their thirteenth birthday—"notwithstanding any parental consent that may have been provided when the individual was a child."[113] Unfortunately, there is a catch with this bill. When information is collected with the assistance of a parent or a parent implies consent by willfully inputting a child's information, it is unlikely the child will be able to delete

106. *Id.*

107. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6505 (1998).

108. Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2013).

109. FTC STAFF REPORT, PROTECTING CHILDREN'S PRIVACY UNDER COPPA: A SURVEY ON COMPLIANCE (2002), https://www.ftc.gov/sites/default/files/documents/rules/children's-online-privacy-protection-rule-coppa/coppasurvey.pdf [https://perma.cc/7WLC-GZY4]; FTC, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FTC (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance [https://perma.cc/5VUX-XYH5].

110. FTC STAFF REPORT, *supra* note 109.

111. Clean Slate for Kids Online Act of 2018, S. 2965, 115th Cong. (2018).

112. *Id.* at § 2(e)(1)(a).

113. *Id.*

the disapproved or unwanted disclosure because of this implicit parental consent.[114]

This bill demonstrates that legislatures, at the very least, understand children under the age of thirteen have a special interest in their privacy and how their information is shared about them on the Internet. But it fails to address any right to recovery for harm or injury resulting from activity carried out specifically by their parents.

In addition to congressional efforts, states have begun to address growing concerns related to individual privacy with respect to their personal information. In June 2018, California introduced its solution with the California Consumer Privacy Act (CCPA), which gives Californians the right to know the type of information companies are collecting from them and provides them with the right to opt out of the sale of their information.[115] For children between the ages of thirteen and sixteen, the parent or child must consent before the company can sell their information.[116] Amendments to the CCPA further clarify when a private right of action may exist; consumers may only file a civil suit against a company if they can claim it was involved in the unauthorized access or disclosure of their personal information.[117] This right is centered around misconduct by a "business," and a private right of action does not appear to exist for those wishing to bring suit against another individual for unapproved disclosure of personal information.[118]

Aside from legislation, U.S. tort law recognizes harms attributable to certain type of communications that constitute an invasion of privacy.[119] The two tort laws typically invoked when a question of privacy arises are Public Disclosure of Private Facts and Publicity Given to Private Life. Public Disclosure of Private Facts exemplifies the invasion of privacy that occurs when parents post information about their children online.[120] Publicity Given to Private Life subjects a person to liability in the event they disclose another's private information in a way that (1) "would be highly offensive to a reasonable person" and (2) "is not of legitimate concern to the public."[121] As discussed below in the following section, constitutional and public policy values may be inconsistent with using this tort law as the foundation of proposed legislation.[122]

---

114. *Id.*
115. CCPA, CAL. CIV. CODE § 1798.120.
116. *Id.* at § 1798.120(c).
117. *Id.* at § 1798.150(a)–(c).
118. *Id.* at § 1798.150(a)(1).
119. Anita Bernstein, *Real Remedies for Virtual Injuries*, 90 N.C. L. REV. 1457, 1458 (2012).
120. *Id.* at 1467.
121. RESTATEMENT (SECOND) OF TORTS § 652D (1977).
122. *Id.* at § 652D special note on relation of § 652D to the First Amendment to the Constitution.

When it comes to restrictive measures, several foreign countries have surpassed the United States with the creation of privacy laws and policies aimed at the general public, including those directed specifically at parents. For example, France is known for its very strict privacy and data protection law, which dates back to the 1978 enactment of "Law 78-17 on Information Technologies, Data Files and Civil Liberties" (78-17).[123] France's law was ahead of its time, anticipating issues to arise in the modern digital era through several amendments, so much so that it is said to have influenced the drafting of the GDPR's personal data protection provisions.[124] French legislation continues to reflect the country's stance with respect to online privacy.[125] More recently, France amended 78-17 with a "right to be forgotten" exclusively granted to minors, which imposes accelerated procedure requirements for online organizations.[126] Before this development, the law did not explicitly differentiate privacy rights of children from those of adults.[127] Thus, this amendment is an example of lawmakers recognizing the distinct need to protect the privacy of children who begin using the Internet at a young age and are vulnerable to the risks associated with that usage.

Although 78-17 does not expressly impose stricter requirements on parents,[128] legal experts have warned French parents "that they should stop posting pictures of their children to Facebook or it could land them in jail years down the line" if the child chooses to take them to court for "breaching their privacy or endangering their security online."[129] These warnings are grounded in the strict nature of France's privacy laws, which may amount to fines for parents or, in severe cases, a sentence of one year in prison for both breaching their child's privacy and endangering their child's online security.[130] The French government is actively aware that images of children can land in the possession of pedophiles or criminals

123. *See* Nicole Atwill, *Online Privacy Law: France*, L. LIBR. CONG. (June 2012), https://www.loc.gov/law/help/online-privacy-law/2012/france.php [https://perma.cc/XQ2K-5JDG].

124. *Id.*

125. *Id.*

126. Loi 2016-1321 du octobre 2016 pour une République numérique [Law 2016-1321 of October 7, 2016 for a Digital Republic], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], October 8, 2016, p. 96 (requiring online organizations to reply to the requester within one month if the requester is a minor, which varies from the two-month allowance when the requester is an adult).

127. Atwill, *supra* note 123.

128. *Id.*

129. Thomas Tamblyn, *French Parents Could Go to Jail for Posting Their Children's Pictures on Facebook*, HUFFINGTON POST U.K. (Mar. 3, 2016), https://www.huffingtonpost.co.uk/2016/03/02/french-parents-could-go-to-jail-for-posting-their-childrens-picture-on-facebook_n_9364998.html [https://perma.cc/3Y8T-WUJG].

130. *Id.*

engaging in identity theft,[131] and it has echoed its distinct interest in protecting children's privacy through the vehicles of widespread communication campaigns and education in schools.[132] Under French law, the initial responsibility of protecting children lies with the parents, not Internet operators.[133]

Similar to Congress's intent with the enactment of COPPA in the United States, the United Nations (UN)[134] and European Commission (EC)[135] also acknowledge the special interest associated with the rights of children. In 1990, the UN adopted the Convention on the Rights of the Child, which acknowledges the importance of a family's well-being while highlighting the heightened need for safeguards and care for the children in particular.[136] Furthermore, Article 3 of the law asserts that all adults should primarily concern themselves with the best interests of children when "making decisions that may affect them."[137] Moreover, the EC takes a specific stance on protecting children through its policy of promoting a safer Internet for them.[138] The EC admits that the Internet can pose certain risks for children and provides resources for Europeans to educate themselves by providing strategies and a specific portal designated for children.[139]

Communities around the globe can, at the very least, agree that children deserve some form of greater protection on the Internet and on activity that affects their development and growth; however, the issue remains complex and the timeline for determining a solution does not appear equal for all jurisdictions. For example, in the U.S., legislators and tort law advocates face constitutional hurdles before they will be able to find a widely accepted resolution consistent with their goals.

131. Chazan, *supra* note 104.

132. Atwill, *supra* note 123.

133. *See generally* Chazan, *supra* note 104.

134. G.A. Res. 44/25, Preamble, Convention on the Rights of the Child (Nov. 20, 1989) (proclaiming that "childhood is entitled to special care and assistance").

135. Accessibility, Multilingualism & Safer Internet (Unit G.3), *Creating a Better Internet for Kids*, EUR. COMM'N: POLICIES (Aug. 23, 2018), https://ec.europa.eu/digital-single-market/en/policies/better-internet-kids [https://perma.cc/E467-TF4P] [hereinafter *Creating a Better Internet for Kids*].

136. G.A. Res. 44/25, *supra* note 134 (defining "children" as people under the age of eighteen).

137. G.A. Res. 44/25, *supra* note 134, at art. 3; *Fact Sheet: A Summary of the Rights Under the Convention on the Rights of the Child*, UNICEF, https://www.unicef.org/crc/files/Rights_overview.pdf [https://perma.cc/4ACG-KUQA].

138. *Creating a Better Internet for Kids*, *supra* note 135.

139. *Id.*

IV. QUASHING FIRST AMENDMENT CONCERNS

In recognizing children's privacy interest in their digital identities, it is also important to recognize parents' interest in their enumerated First Amendment right to freedom of speech that, at a first glance, can apply to their online disclosures and activity. While children's privacy interests should not be ignored, it has long been accepted that "Congress shall make no law . . . abridging the freedom of speech."[140] United States citizens value this fundamental principle that prohibits any law compelling self-censorship, even when legislative attempts are intended to curb offensive or destructive communication directed at children.[141]

Under a tort theory, the Supreme Court has held that the First Amendment bars recovery for those claiming invasion of privacy under the tort of Publicity Given to Private Life when it involves disclosure of facts that are a matter of public record.[142] The Court did suggest that a limited category of expression may exist which is "of such slight social value as a step to truth that any benefit derived from them is clearly outweighed by the social interest in order and morality."[143]

However, the Court has made general damages hard to recover for plaintiffs asserting an invasion of privacy claim.[144] In *Gertz v. Robert Welch, Inc.*, the Court concluded that the common law rule providing for presumed and punitive damages motivates self-censorship and is thus inconsistent with the First Amendment.[145] On the other hand, unreasonable disclosure of private facts may allow compensatory recovery for one's emotional distress, and the Constitution does not require proof of damage to one's reputation before such damages can be awarded.[146]

Under the legislative route, case law continues to suggest that the First Amendment right stands strong, even in the digital age. In1997, the Supreme Court decided in *Reno v. American Civil Liberties Union* that Internet speech may be awarded the same First Amendment protection given to traditional speech.[147] The Court held in favor of plaintiffs who challenged the provisions of the Communications Decency Act (CDA), an act that sought to criminalize certain Internet speech to protect children under eighteen from obscene or "indecent" or "patently offensive"

---

140. U.S. CONST. amend. I.

141. Melissa A. Whitehead, Note, *MySpace, WhoseSpace? The Impact of Semi-Private Social Media on Threats and the First Amendment*, 39 NEW ENG. J. CRIM. & CIV. CONFINEMENT 193, 198–99 (2013).

142. Cox Broad. Corp. v. Cohn, 420 U.S. 469, 494–95 (1975).

143. *Id.* at 495.

144. Bernstein, *supra* note 119, at 1473.

145. Gertz v. Robert Welch, Inc., 418 U.S. 323, 349 (1974).

146. RESTATEMENT (SECOND) OF TORTS § 621 cmt. b (1977).

147. Reno v. Am. Civil Liberties Union, 521 U.S. 844, 849 (1997).

communications sent via telecommunications devices or computers.[148] The Court concluded that the act was unconstitutional because its broad restrictions did not serve a narrowly tailored governmental interest, and effective but less restrictive alternatives existed.[149]

In *Ashcroft v. American Civil Liberties Union*, the Court similarly struck down the restriction of content-based speech codified in COPPA.[150] In 2004, by way of COPPA, Congress attempted to penalize Internet speech that involved the publication of any obscene material, including photographs,[151] and imposed a fine and prison sentence for those who knowingly posted content online, for commercial purposes, that is harmful to children.[152] The Court agreed with the District Court ruling that less restrictive methods existed, "particularly blocking or filtering technology."[153] The Court reasoned that these methods were not unconstitutional because they imposed selective speech restrictions for those on its receiving end—not absolute speech restrictions for its source.[154]

During oral arguments of a more recent case, *Packingham v. North Carolina*, the justices appeared to agree that "access to social media is worthy of constitutional protection."[155] The case involved a sex offender challenging a North Carolina statute that prohibited him from accessing social media sites, and the Court held in his favor on First Amendment grounds.[156] The Court reasoned that social media provides a way to gain information and "communicate with one another about it on any subject that might come to mind."[157] Barring the sex offender's ability to access those websites would essentially keep him from what many consider the "principal sources for knowing current events, checking ads for employment, [and] speaking and listening in the modern public square."[158] We must then consider the following question: if a sex offenders' online

148. *Id.* at 868.

149. *Id.* at 846 (finding that user-based software available at the time suggested that a "reasonably effective method by which *parents* can prevent their children from accessing material which the *parents* believe is inappropriate w[ould] soon be widely available").

150. Ashcroft v. Am. Civil Liberties Union, 542 U.S. 656, 660 (2004).

151. Whitehead, *supra* note 141, at 202.

152. *Ashcroft*, 542 U.S. at 656 (attempting to impose a $50,000 fine and six-month prison term for violations).

153. *Id.*

154. *Id.* at 657.

155. Ephrat Livni, *A US Supreme Court Discussion of Free Speech and Social Media Got Comically Postmodern*, QUARTZ (Mar. 3, 2017), https://qz.com/922444/a-us-supreme-court-discussion-of-free-speech-and-social-media-got-comically-postmodern/ [https://perma.cc/77GT-2X6A].

156. Packingham v. North Carolina, 137 S. Ct. 1730, 1738 (2017).

157. *Id.* at 1737.

158. *Id.*

activity is currently awarded constitutional protection by the U.S. court system, how might privacy advocates convince Congress and U.S. courts that parental online activity should be restricted when it compromises a child's right to privacy?

The answer to this question should lie in a very significant distinction: so far, the Supreme Court has struck down legislation that sought to restrict certain expressions of information *directed at* children, not the expression *of* children's personal information itself. In other words, the condemned legislation has not tried to restrict people from expressing and speaking about children; the efforts stem from the desire to restrict expressing harmful information directly to children. North Carolina, for instance, was not trying to restrict certain individuals from posting children's personal information; rather, it was trying to restrict them from accessing children's information or communicating with children. In *Packingham*, the Supreme Court essentially stated that social media is a public forum, and any information shared on it, including children's information, is treated as public information.[159]

The Court has also barred recovery under tort theory on constitutional grounds for disclosures of information that is of public record or concern.[160] While there may be a compelling interest in protecting information beyond political and newsworthy information, such as general information about daily life,[161] no compelling reason exists for why children's sensitive information should be of value to the public—specifically the combination of sensitive information found online that could result in harm to a child. For instance, no likely harm would stem from a parent sharing valuable information about their child and parenting experience to the public, so long as it is expressed in a reasonable way that leaves the specific child anonymous and free from the potential harms of oversharing.[162]

Furthermore, consider the scenario that often occurs when paparazzi or other people in the public snap a photograph of a nearby celebrity and their young child and post it online. Such individuals are far removed from the stranger child and are less likely to consider the risks to his privacy. It may be understandable—albeit disturbing—why someone unrelated to a child would give up their interest in their fundamental right to freedom of speech over any interest in that child's safety and protection for economic reasons.

---

159. *See id.*

160. *See generally* Cox Broad. Corp. v. Cohn, 420 U.S. 469, 495 (1975).

161. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1092–93 (2000).

162. Keith & Steinberg, *supra* note 18, at 413.

On the other hand, one would expect that a child's parents would want to protect their child's information in most instances because of the typical guardian relationship that exists between parents and their children. Parents are inherently the guardian of their children's information in a myriad of other scenarios that require external parties to receive permission before obtaining information from their children.[163] They should not value the protection of that information any less when posting information on websites like social media that arguably reach far more estranged viewers than those in typical forums where such information is shared, such as with school administrators or extracurricular activities. If individuals with ill-intentions, such as sex offenders, are constitutionally protected and permitted to access websites containing children's personal information, the parents must act as the barriers between these individuals and their children as the keepers of such information.

The potential reach that online posting poses justifies limiting what should be protected by the First Amendment's right to freedom of speech. Demands for more legal protection come with each new device or technology that is introduced that "makes sharing content easier."[164] These demands undoubtedly implicate people's "privacy, . . . freedom of speech, and . . . the structure of . . . participatory democracy."[165] Therefore, the powerful, communicative nature of today's Internet warrants a new perspective on the fundamental right of freedom of speech, at least as it relates to protecting children's right to privacy in their digital identities, for the reasons discussed in Part II. Critics who believe in keeping our enumerated rights immune from legislative change place heavy weight on the Framer's intent and purpose when drafting our Constitution.[166] While entitled to their belief, these originalists should acknowledge the following quote by Thomas Jefferson:

> Laws and institutions must go hand in hand with the progress of the human mind, as that becomes more developed, more enlightened, as new discoveries are made, new truths are discovered and manners

163. *See generally* Erika Elmuts, *Please Stop Posting Pictures of My Child on Facebook*, CONSCIOUS PARENTS, http://www.consciousparents.org/stop-posting-pictures-of-my-child-online-please/ [https://perma.cc/E53W-QBTX].

164. ROBERT BRAUNEIS & ROGER E. SCHECHTER, COPYRIGHT: A CONTEMPORARY APPROACH 1 (2d ed. 2018).

165. *Id.*

166. JOHN H. GARVEY ET AL., MODERN CONSTITUTIONAL THEORY: A READER 91 (5th ed. 2004).

> and opinions change. With the change of circumstances, institutions must advance also to keep pace with the times.[167]

Others with ideology akin to Jefferson suggest that society might need to rethink the First Amendment in the digital era as the public surely has become "more enlightened" on the power and effects of advancing technology.[168] While the possibilities of the early Internet may have embodied the right's purpose to "protect and foster a democratic culture," the modern digital age allows for a far greater reach and loopholes for routing around traditional ways of fostering culture.[169]

In this context, the First Amendment's original purpose may no longer be served.[170] Further, narrowly limiting—not depleting—parents' content-based speech solely on online mediums to ensure greater protection of children's privacy should not be understood as hindering this fundamental purpose of the First Amendment's right to freedom of speech. Overall, no compelling reason exists for why children's sensitive information should be of value to the public. Therefore, even though the Supreme Court has opened the door to argue that children's information constitutes public, and thus, constitutionally protected information if shared by a parent, such view should ultimately be rejected.

V. A BALANCED CIVIL RIGHT AND REMEDY

While current legislation touching on biometrics and children's general online safety is an admirable first step, the United States needs federal legislation specifically directed at protecting children's right to privacy in their sensitive personal information. Using a tort-based approach, Congress should propose a law that aims to narrowly limit parental disclosures of their children's sensitive personal information via online platforms that would allow for a private right of civil action by their child, aged sixteen or older[171] due to actual resulting harm. This type of restricted speech should be limited to only certain content, exposed in such a distinct way, which has the reasonably foreseeable potential to directly cause a legally cognizable injury, as set forth by the law's provisions—

---

167. Thomas Jefferson to Samuel Kercheval (July 12, 1816), *in* THOMAS JEFFERSON PAPERS: GEN. CORRESPONDENCE (Library of Cong. n.d.), https://www.loc.gov/item/mtjbib022494/ [https://perma.cc/6XXX-X4HQ].

168. *See generally* Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149 (2018) (discussing the problems of free speech resulting from communication technology).

169. Id.

170. *Id.* at 1152.

171. California Consumer Protection Act (CCPA) of 2018, CAL. CIV. CODE § 1798.120(d) (West 2020) (mirroring CCPA's age acceptable for child consent by defining eligible child claimants as those aged 16 or older).

parental liability which could only surface in the event that a child seeks a remedy of compensatory damages or injunctive relief for such injury. Although the proposed legislation should not completely ignore parents' feelings about potential adverse action by their own children, persuasive policy reasons should ultimately overcome any hurdles regarding the restriction of such parental action.

A majority of parents claim to feel comfortable about something being posted about their child on social media, while only a small minority admit to ever asking family members or friends to remove content posted about their child.[172] But, they are overlooking that the right to privacy is one that does not "matter until it matters."[173] And, a right without a remedy is of little value to those who are powerless in asserting it until they are old enough to recognize its breach by the very people who did not appreciate its worth. Because studies show that parents are not instinctually wary about loosely sharing their child's information, changing their minds will take more convincing than any social media campaign could achieve.

Even though there are policy reasons supporting parental immunity from suit for injuries by a child, persuasive reasons exist for disregarding parental immunity in the context of a child's right to privacy.[174] Of the reasons in favor of parental immunity, keeping the peace by avoiding "interference with parental discipline, care and control" appear to be those most offered by relevant court decisions.[175] However, other courts acknowledge these reasons as outdated and take the position that the interest in protecting individuals in society from harm outweighs any possibility of familial discord.[176] Of course, permitting children to bring action against their parents should only apply to the special circumstances discussed above, which amount to unreasonable parental discretion with respect to caring for their children.[177] In other words, sharing a photograph of one's child in a state of undress that also discloses intimate health information on one's public profile does not amount to parental action reasonably necessary in caring for a child.[178]

---

172. Duggan et al., *supra* note 15.

173. Aisha Sultan & Jon Miller, *'Facebook Parenting' Is Destroying Our Children's Privacy*, CNN (May 25, 2012), https://www.cnn.com/2012/05/25/opinion/sultan-miller-facebook-parenting/ [https://perma.cc/N42N-72GM].

174. *See generally* 2 STUART M. SPEISER ET AL., AMERICAN LAW OF TORTS § 6:49 (Supp. 2019).

175. *Id.* (attributing depletion of family assets at the expense of other children, inevitable inheritance by the parents of the recovered amount, and danger of fraud and collusion as the other main policy reasons).

176. *Id.*

177. *Id.*

178. *See* Caroline E. Johnson, Comment, *A Cry for Help: An Argument for Abrogation of the Parent-Child Tort Immunity Doctrine in Child Abuse and Incest Cases*, 21 FLA. ST. U. L. REV. 617,

Currently, no comprehensive federal law exists that protects children's right to privacy by restricting certain adult speech on the Internet. Rather, the United States has taken a sectoral approach when it comes to children's privacy, such as the collection of private information online and child pornography prohibitions.[179] Each of the sectoral approaches illustrates society's general principle of recognizing the unique and vulnerable nature of the child population as a protected class; however, none of these laws aim to protect children's privacy by restricting speech of those with the greatest control over a child's private information: their parents or legal guardians. Rather, existing laws target and place restrictions on other unreliable bad actors while simultaneously providing some immunity from liability to some online "intermediaries," such as social media platforms and commercial websites.

Under § 230 of the United States Code, if a sex offender posts images of child pornography to Facebook, the sex offender is held liable for the image, not Facebook.[180] One could argue that the solution should be to repeal such intermediary immunity and impose liability directly on to the computer service provider who is best suited for controlling what information is shared or disclosed on its platform. However, the policy behind § 230's immunity supports the argument behind placing such restriction and liability on someone else because it increases the flexibility and power of the intermediaries that continue to foster society's growth and progress.[181]

Instead, an equally strong policy argument supports the choice behind starting right at the source to restrict and impose liability on the parents who are the next closest thing to the owners of children's private information. The online service providers and social media platforms should be focused on furthering the interests of their users overall instead of being burdened with focusing on one category of users. It would be far more efficient to inflict such restrictions on the parents themselves who arguably should be focused on protecting and furthering the interests of their children.

Although the FTC has recognized that "the role of parents in protecting their children's privacy is fundamental" to engaging in "fair information practice[s]," it has only applied this fundamental duty to overseeing and restricting actions and disclosures by the children directly,

---

634 (1993) (discussing a case that abrogated parent-child immunity in automobile accidents because such accidents do not implicate parental authority or discretion in child care).

179. *Boyd*, *supra* note 72, at 179–80.

180. *See id.* at 184.

181. *Id.*

not by the parents themselves.[182] Therefore, the absence of regulations incentivizing parents to refrain from oversharing children's private information online, coupled with the lack of recourse for children harmed by such sharing, highlights the need for new and increased regulation in the arena of children's privacy on the Internet.

This proposed legislation should reconcile certain aspects of existing legislation, both in the U.S. and abroad, and incorporate qualities to distinguish itself from previously failed congressional proposals. The legislation should incorporate the CCPA's prohibition limiting third party disclosures of children's sensitive information, account for non-commercial parental disclosures, and define "children" as people thirteen or younger.[183] The bill should mirror the UN's efforts to expressly state the need for a heightened interest in protecting children and follow in France's footsteps to allow children to retroactively file suit against their parents but keep parental liability limited to civil rather than criminal liability. In addition, the compensatory damages for surviving privacy invasion claims resulting in emotional distress or identity theft and injunctive relief for those wishing to remove content previously posted by one's parent.

The new legislation would be distinguishable from the legislation struck down in *Reno* for its broad suppression of speech because it should provide the specific scenarios and combinations for what is and what is not permitted to overcome First Amendment objections. In *Reno*, the legislation restricted directing generally "patently offensive" communications toward children in order to protect them from harmful material.[184] Rather, this Comment argues for legislation that is acutely specific in regard to what combinations of sensitive personal information and sharing methods may or may not be disclosed and used by parents in order to protect the right to privacy.

For instance, it may be safe to share a photograph of a child on one's private account of which information is only shared with others whom the parent has thoughtfully accepted as followers. Perhaps photographs may be acceptable under this scenario so long as other sensitive information is not attached, such as a full name, birth date, or geolocation information. Parents often carelessly include birth dates, middle names, and health updates in their captions, which can aid hackers and identity thieves.[185] To determine what information is the most vital to protect, pediatricians could

182. MARTHA K. LANDESBERG ET AL., FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 37 (1998).

183. CCPA, CAL. CIV. CODE § 1798.120(d) (West 2020).

184. Reno v. Am. Civil Liberties Union, 521 U.S. 844, 845–46 (1997).

185. Milian, *supra* note 94.

educate legislators on what types of other psychosocial information should be restricted and up until what age to ensure healthy and autonomous identity development.[186]

In certain circumstances, as with celebrities, where sensitive information may already be known to the general public because of publicity in the news or when the parent's account is already made public, perhaps the answer rests in encouraging the use of certain filters or masking mechanisms that could block biometric risks associated with images[187] that are often forwarded and re-shared by strangers. Technical biometric experts would be needed to ascertain the exact combinations and altering mechanisms that could help circumvent the apprehended risks associated with cybersecurity and identity theft.

Again, as with both general public and celebrity disclosures, parents should be restricted from sharing sensitive information not previously known to the public, such as a child's location, photographs of children in a state of undress, or psychosocial information. These restrictions can aid in combatting the concerns associated with cybersecurity, child predators, and identity development. With respect to the virtual predators in the form of pedophiles and users of child exploitation sites, research would be needed to show how the material is typically sourced and whether images are typically taken from public profiles or private profiles through hacking. Yet, since the legislation should provide children with a right to remedy a cognizable injury, it should encourage parental use of measures to protect images rather than provide for their absolute prohibition (aside from those of children in a state of undress, as mentioned above).

Critics may argue that disclosures of children's sensitive personal information are often inevitable—consider magazines and news stories that are published online or broadcasted on television. While this point holds some truth, parental restrictions can help to impede third parties from easily gaining sensitive information, thus preventing the snowball effect and greater viral exposure.[188] In fact, other family members or close friends often share baby pictures, sometimes provided by the parents, on social media to viewers and followers whom the parents are unaware.

---

186. Pediatricians recommend that parents keep children anonymous when sharing struggles and give older children "veto power" when it comes to online sharing. Keith & Steinberg, *supra* note 18, at 414.

187. *See generally* Korolov, *supra* note 65 (suggesting that biometric identification technology might fail to recognize someone wearing makeup or glasses); *see also Biometrics & Image Processing*, TUTORIALS POINT, https://www.tutorialspoint.com/biometrics/biometrics_and_image_processing.htm [https://perma.cc/E4A8-JXSC] (explaining that image-based biometrics require clear and unadulterated versions of images to successfully work).

188. *See* Bernstein, *supra* note 119, at 1457 (emphasizing the effect of online communication's ability to reach more people and cause more harm than similar spoken or written communications).

Once the content is no longer under the exclusive control of the parents, deletion at some later date in the future becomes far trickier for concerned parents or children.[189] For this reason, this Comment argues that there is no more effective, less restrictive alternative to the proposed legislation, which incentivizes parents to take precautionary measures as the gatekeepers of information to protect their children's privacy.

Lacking such an alternative makes this proposal distinguishable from the legislation struck down in *Ashcroft v. ACLU*.[190] There, the legislation aimed to protect children from harmful material by restricting the general adult population's speech, but an alternative was that concerned adults could use filtering or blocking technology to protect and censor their children from the information.[191] Here, no similar alternative exists that would more effectively serve the goal of protecting disclosure of information about children, and thus children's privacy.

Some legal scholars instead suggest education and an increased awareness through mass marketing campaigns about the growing concerns associated with children's right to privacy.[192] However, the formal enactment of legislation would more effectively incentivize parents to respect their children's privacy rights in ways that a general increase in awareness cannot. Many parents are naïve and believe that privacy will never become a problem for them because they do not think they have anything to hide.[193] Therefore, lawmakers need to effectively discourage the type of activity that is hard to reverse years later once the harm is realized. Because this legislation would be narrowly tailored around selective parental restrictions to protect those children actually affected by a cognizable injury, no less restrictive alternative is possible.

Lastly, the legislation should prescribe a cause of civil action against the parents for a child's right to privacy rather than against the third party online operators. Some people in the legal community tend to put the burden of protecting people's information onto the private technology industry as the ultimate collectors, users, and sellers of online personal information.[194] For instance, technology entities could stop enabling biometric identification technology vulnerable to misuse and identity theft. However, both government and private industries have already made significant investments in biometric technology, and its use comes with

189. Milian, *supra* note 94.

190. Ashcroft v. Am. Civil Liberties Union, 542 U.S. 656, 673 (2004).

191. *Id.* at 666–67.

192. *See, e.g.,* 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, 174–75 (2016).

193. Sultan & Miller, *supra* note 173.

194. *See* McKenna, *supra* note 59, at 1075–79.

many financial benefits.[195] Moreover, general restrictions imposed on businesses generally fail to serve a narrow interest, which the Supreme Court is unlikely to uphold based on historical precedent. Instead, imposing selective restrictions onto the narrow group of parents would provide protection for children as a special-interest group without restricting disclosures of personal information about a knowingly consenting adult. Thus, the benefits of biometric technology could still be realized with respect to adult-biometric data.

Besides, the proposed legislation providing a remedy for children in an action against their parents would be a catch-all solution to prevent more issues than just those associated with sensitive information misused in biometric technology. Legislation restricting information shared by parents at the source also serves to protect from other concerns about psychosocial development and a child's general right to privacy in their information. Not to mention, the illegal use of biometric technology would be much harder to regulate than affirmative acts made by parents, which comes along with the evidentiary benefit of the specifically disapproved content.

Most importantly, it should be theoretically easier to convince parents to abstain from potentially harmful activity than a removed third party organization. Children are vulnerable in ways that their adult parents are not.[196] Parents offer the first layer of protection when it comes to their children; they are best suited to act as stewards of their children's rights until the children have matured enough to protect their interests on their own.[197] Parents are the initial keepers and sources of sensitive information; therefore, legislation should aim to mitigate risks to privacy of children's sensitive information by inflicting liability onto the parents as the willing sources of the information rather than the unintending online operator.

195. *Id.* at 1067.

196. Simone van der Hof, *I Agree . . . or Do I?: A Rights-Based Analysis of the Law on Children's Consent in the Digital World*, 34 WIS. INT'L L.J. 409, 434–36 (2016).

197. Sorensen, *supra* note 192, at 171.

CONCLUSION

Social media has created a space for average citizens to gain rapid exposure and for public figures to achieve exponentially greater publicity. While adults are afforded the freedom to communicate and share information about themselves, they should not be afforded the same freedom with respect to information about children. Rather, the creation of an individual's digital identity, as one comprised of sensitive information, should be preserved so every individual can autonomously develop and control his or her self-image. Yet, the growing trend appears to involve parents' careless sharing of every intimate detail online. Legal recourse for detrimentally affected children would be the most influential solution to spark the reversal of such a dangerous parental tendency.