

5-20-2022

Marketing Research and Children's Consumer Privacy Rights: A Battle in the Digital Age

Hadley Johnson

Barry University School of Law

Follow this and additional works at: <https://lawpublications.barry.edu/cflj>



Part of the [Family Law Commons](#), [Juvenile Law Commons](#), and the [Other Law Commons](#)

Recommended Citation

Johnson, Hadley (2022) "Marketing Research and Children's Consumer Privacy Rights: A Battle in the Digital Age," *Child and Family Law Journal*: Vol. 10: Iss. 1, Article 5.

Available at: <https://lawpublications.barry.edu/cflj/vol10/iss1/5>

This Article is brought to you for free and open access by Digital Commons @ Barry Law. It has been accepted for inclusion in Child and Family Law Journal by an authorized editor of Digital Commons @ Barry Law.

Marketing Research and Children's Consumer Privacy Rights: A Battle in the Digital Age

Cover Page Footnote

HADLEY JOHNSON, Candidate for J.D., Barry University, Dwayne O. Andreas School of Law, May 2023. I would like to thank my parents for their unwavering support in all my endeavors. Thank you to everyone who made this Note possible, especially my Editor-in-Chief and Note and Comment Editor. Finally, I would like to thank Professor Wes Henricksen for overseeing this Note.

Marketing Research and Children’s Consumer Privacy Rights: A Battle in the Digital Age

*Hadley Johnson**

ABSTRACT

Advancements in technology and social media have led to a decreased level of personal data privacy. Companies are now provided with limitless ways to extract information about their customers, even without their knowledge. This is especially concerning when it is the personal information of a child that is being collected, as in the United States, few regulations exist to protect them on social media. Even fewer regulations exist to protect children between the ages of thirteen and seventeen. The purpose of this Note is to discuss the importance between market research practices and children’s consumer privacy rights in the digital age. This Note discusses proposed solutions including adopting the United Nations Convention on the Rights of a Child to better protect children ages thirteen through seventeen, as well as reforming the current Children’s Online Privacy Protection Act, and criticism of parental control.

INTRODUCTION.....	155
BACKGROUND.....	156
A. What is Marketing Research?.....	158
B. Consumer Privacy Rights vs. Children’s Privacy Rights.....	159
LEGAL ISSUES	161

* Candidate for J.D., Barry University, Dwayne O. Andreas School of Law, May 2023. I would like to thank my parents for their unwavering support in all my endeavors. Thank you to everyone who made this Note possible, especially my Editor-in-Chief and Note and Comment Editor. Finally, I would like to thank Professor Wes Henricksen for overseeing this Note.

2022]	<i>CHILD AND FAMILY LAW JOURNAL</i>	155
	A. Children’s Lack of Right to Privacy Under Parents’ Right to Care, Custody, and Control	162
	B. Duty to Read Rule	164
	C. Rise of TikTok and the Concerning “For You Page” Data Collection Algorithm	165
	D. Current Digital Privacy Initiatives	168
	E. Implications for Market Research Practices	168
	SOLUTIONS.....	170
	A. The United Nations Convention on the Rights of a Child	170
	B. Importance of Reforming the Children’s Online Privacy Protection Act	171
	C. Criticism of Parental Control.....	174
	CONCLUSION.....	176

INTRODUCTION

The increase in technology and social media led to a decreased level of consumer privacy. Companies are provided with limitless ways in which to extract information about their customers. With the current generation being raised by technology, children and their privacy rights have ultimately become caught in the crossfire. This Note will discuss the relationship between market research and children's privacy rights in the digital age. This Note will discuss the background of marketing research; children’s privacy rights, including the Fourth Amendment issue implicated through the rise of technology; the development of digital privacy initiatives; and the policy considerations and proposed solutions of current market research practices on children through technology and social media.

Part II of this Note discusses the background of marketing research practices, including what they are, how they have evolved with the rise in technology, and the consumer and children's privacy rights that exist (or do not exist) with these practices. Part III discusses the legal issues implicated through a lack of right to privacy under: (1) parents’ right to care, custody, and control, (2) the duty to read rule, (3) the rise of the social media phenomenon “TikTok” and the impact of its “For You Page” data collection algorithm, (4) the current digital privacy initiatives

that exist to combat the issue, and (5) the implications of these initiatives for market research practices. Part IV discusses the proposed solutions including adopting the United Nations Convention on the Rights of a Child (“UNCRC”), reforming the current Children’s Online Privacy Protection Act (“COPPA”), as well as the criticisms of parental control. Part V discusses the conclusion to these legal issues and my recommendation on how to improve as society moves forward, with the continuing advancement of technology and social media.

BACKGROUND

The main consequence that arises from the collection of digital data through digitized marketing research practices is that consumers are worried about the extent to which their information is being collected.¹ This issue results from the increased use of marketing methods that provide the “intimacy close contact [which] smaller markets require[.]”² These techniques rely on continuous learning of the consumer, which are often “rich, descriptions of personal behavior that indicate wants, needs and the best way to satisfy them are more valuable than estimates of characteristics based on large samples, particularly when the variation estimate is high.”³ This type of continuous collection of detailed data leads consumers to the feeling of intrusion, as “[i]nformation [] provid[ing] a competitive advantage is not likely to be in the public domain.”⁴ This also leads to concern about personal information falling into the hands of those outside of the company and being used to harm the consumer.⁵ With the use of technology for gathering, processing, and analyzing, this personal information can be collected with or without the knowledge of the consumer.⁶ When technology is used to obtain personal data to profile consumers without their knowledge, “the threats to consumer information privacy in a networked world are considerable.”⁷ This is especially troubling when the personal data belongs to a *child*.

¹ See Frank Franzak et al., *Online Relationships and the Consumer’s Right to Privacy*, 18 THE J. OF CONSUMER MKTG. 631, 632 (2001).

² *Id.* at 631.

³ *Id.* at 631-32.

⁴ *Id.* at 632.

⁵ *Id.*

⁶ *Id.*

⁷ Frank Franzak et al., *Online Relationships and the Consumer’s Right to Privacy*, 18 THE J. OF CONSUMER MKTG. 631, 633 (2001).

For example, family consumer favorites, such as Target, collect personal information without consumers' direct knowledge.⁸ Target uses data mining techniques to direct specific coupons and flyers to consumers based on their buying behaviors.⁹ Specifically, they use this information to develop a "pregnancy score" based upon a consumer's buying patterns, which aids in distributing coupons and flyers for products that soon-to-be moms would need.¹⁰ What disturbs consumers is when they receive these targeted promotions in advance, without ever disclosing to the company that they are pregnant.¹¹ This technique was particularly intrusive when a high school girl received coupons in the mail for baby products, only to be found by her father, who was unaware of her pregnancy.¹² It is concerning for a large company to be more knowledgeable on intimate details about a child than their own family, and further demonstrates the need for action to further protect children.

Digital marketing has been rapidly evolving, but ways in which to regulate it have been developing at a slower pace.¹³ The Federal Trade Commission ("FTC") promotes a self-regulation method to protect consumers from the "spying" of big companies.¹⁴ Their industry guidelines include: notice, the right for the consumer to be notified of what the company will do with their information; choice, the right for the consumer to decide if their data will be collected; access, the right for the consumer to view the information that has been collected; security, the expectation that the company will protect consumer information; and redress, self-regulation or governmental regulations to enforce.¹⁵ Other initiatives recommended by the FTC include the National Association of Criminal Defense Lawyers Fourth Amendment Center.¹⁶ While these solutions provide guidance for parents regarding their children's privacy rights, this Note proposes further regulation to work in tandem with COPPA. Ideally, these solutions would be enforced by the FTC, thus

⁸ Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?searchResultPosition=1>.

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

¹³ See Franzak, *supra* note 1, at 641.

¹⁴ *Id.* at 639.

¹⁵ *Id.*

¹⁶ *Id.*

providing a direct focus and protection to children's privacy rights from online marketing research.

A. What is Marketing Research?

Marketing research is the method used by marketers to collect an array of data that is useful to a company in soliciting business.¹⁷ Marketers have shifted their strategy to focus more on relationship marketing.¹⁸ This marketing technique provides companies with more detailed descriptions of personal behavior by uncovering customer-specific wants and needs.¹⁹ In having this information, marketers are able to decide the best way in which to satisfy these wants and needs.²⁰ This type of specified and personalized information provides far more value as opposed to characteristics of an overall large sample, as it leads to long-term buyer-seller relationships.²¹

Various methods can be used to collect this type of data. Since marketing research has evolved into a procedure that desires a focus on smaller, more detailed markets, new methods have become commonly used.²² Companies have implemented techniques, such as interactive marketing, one-to-one marketing, and customer relationship management models, in order to extract the valuable data that stems from individualized marketing research.²³ This customer profile information "provides an advantage in a competitive marketplace, where knowledge about the target buyer needs to be more detailed, more personal, increasingly timely, and preferably, exclusive."²⁴ The rise in technology has increased the ability of marketers to obtain this personal information.²⁵

The growth of technology in the marketing research field has led to privacy concerns.²⁶ The main consequence that arises from the use of the digital world in relationship marketing research practices is that

¹⁷ *Id.* at 631-32.

¹⁸ *Id.* at 639.

¹⁹ Frank Franzak et al., *Online Relationships and the Consumer's Right to Privacy*, 18 THE J. OF CONSUMER MKTG. 631, 639 (2001).

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

²³ *Id.*

²⁴ *Id.*

²⁵ Frank Franzak et al., *Online Relationships and the Consumer's Right to Privacy*, 18 THE J. OF CONSUMER MKTG. 631, 632 (2001).

²⁶ *Id.*

consumers are worried about the extent of their information being collected.²⁷ The feeling of intrusion stems from the idea that “information that provides a competitive advantage is not likely to be in the public domain.”²⁸ This also leads to the concern of personal information falling into the hands of those outside of the company and being used to harm the consumer.²⁹ With the use of technology for gathering, processing, and analyzing, this personal information can be collected with or without the knowledge of the consumer.³⁰ As the next section demonstrates, when technology is used to obtain personal data to profile consumers without their knowledge, it infringes upon their consumer privacy rights.³¹

B. Consumer Privacy Rights vs. Children’s Privacy Rights

When the collection of personal information by companies is “invisible” to consumers, they are infringing upon consumer privacy rights.³² This unknown and non-consenting method of personal data collection is not consistent with public policy considerations³³ and American appreciation behind the Fourth Amendment.³⁴ The Fourth Amendment guarantees American citizens protection from governmental unreasonable searches and seizures.³⁵ Although most of these companies are private actors, the *concept* of “feeling safe in the sanctity of your own home”³⁶ and the spirit of the Fourth Amendment can extend to the collection of consumer information, as consumers should have a reasonable expectation of privacy to their personal data. Technological

²⁷ *Id.*

²⁸ *Id.* at 639.

²⁹ *Id.*

³⁰ *Id.*

³¹ Frank Franzak et al., *Online Relationships and the Consumer’s Right to Privacy*, 18 THE J. OF CONSUMER MKTG. 631, 639 (2001).

³² *Id.*

³³ *Id.* at 632.

³⁴ See Nation’s Criminal Defense Bar Launches Initiative to Educate, Litigate Privacy Challenges in a Digital Age, PROQUEST (Apr. 24, 2018), <https://www.proquest.com/docview/2030166399?accountid=27715&parentSessionId=pLqQe6Mq78qX1glpPkt5AZVgmW2c5PKG18coWe9GaIk%3D>.

³⁵ *Id.*

³⁶ See U.S. CONST. amend. IV; see also, *When the Fourth Amendment Applies*, FINDLAW (Feb. 5, 2019), <https://www.findlaw.com/criminal/criminal-rights/when-the-fourth-amendment-applies.html>.

advancements have become a secret and automatic way for companies to collect data on the consumer, in order to create a customer profile.³⁷ These profiles are made up of personal information that was obtained without consent and without direct knowledge to the consumer, therefore invading privacy but not destroying the expectation of it.³⁸

Even some consumer favorites, such as Target, collect personal information without their direct knowledge.³⁹ Target is a primary example of a large, popular company that profiles customers in an effort to target specific promotions.⁴⁰ Target assigns each customer a “guest identification number.”⁴¹ This is linked to their name, credit card, or e-mail address and keeps track of their purchase history, as well as any demographic information collected or even acquired from other sources.⁴² Through these data mining techniques, Target can direct specific coupons and flyers to consumers based on their buying behaviors.⁴³ This is the reality, and even *expectation*, in today’s world of consumerism.

With technology, the average consumer’s view toward privacy has changed over generations. Marketers could not have done what they do today with previous generations, as the intricate access that technology provides was not available until recently.⁴⁴ In the early to mid-1900s, a study took America by surprise when ⁴⁵William Herbert Sheldon, an American psychologist who directed an institute for physique studies at Columbia University, conducted an experiment to research the three body types.⁴⁶ His methods to collect data were controversial because he used subjects from America’s most prestigious institutions, such as Harvard and Yale.⁴⁷ Students at these universities were asked to strip

³⁷ See Franzak, *supra* note 1, at 639.

³⁸ *Id.*

³⁹ Duhigg, *supra* note 8.

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.*

⁴³ *Id.*

⁴⁴ See Franzak, *supra* note 1.

⁴⁵ Ron Rosenbaum, *The Great Ivy League Nude Posture Photo Scandal: How Scientists Coaxed America’s Best and Brightest Out of Their Clothes*, N.Y. TIMES MAG. (Jan. 15, 1995), <https://www.nytimes.com/1995/01/15/magazine/the-great-ivy-league-nude-posture-photo-scandal.html>.

⁴⁶ *Id.*

⁴⁷ *Id.*

down, so scientists could photograph their posture.⁴⁸ The controversy with this study was that the students were never asked for their consent to participate, nor were they informed of the purpose of their photographs.⁴⁹ The study was criticized as an infringement upon the students' privacy, due to the failure to obtain their consent, similar to the way digitized marketing infringes on privacy rights today.⁵⁰

With data collection via technology, consumers can be unaware of this ongoing procedure,⁵¹ yet more information is in reach for companies, posing a bigger threat.⁵² The digital world essentially places every aspect of a consumers' life into the hands of a third party.⁵³ Social media and internet usage have certainly made an impact as "[t]he aggregation and correlation of data from various sources make it increasingly possible to link supposedly anonymous information to specific individuals and to infer characteristics and information about them."⁵⁴ The result is that today, "a widening range of data has the potential to be personal information, i.e. to identify us uniquely."⁵⁵ The digital world has created privacy threats that were not possible in previous generations—and is only going to get more precise as technology advances.

LEGAL ISSUES

Several legal issues pose difficult hurdles when it comes to navigating the technological advancement of market research practices.⁵⁶ Its impact on children's privacy rights, specifically, makes it challenging to develop a solution centered around protection due to several legal principles.⁵⁷ Children's rights in general are quite limited under the

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ See Duhigg, *supra* note 8.

⁵² See Franzak, *supra* note 1.

⁵³ Cameron F. Kerry, *Why Protecting Privacy is a Losing Game Today—And How to Change the Game*, BROOKINGS (July 12, 2018), <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/>.

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ See Franzak, *supra* note 1, at 635.

⁵⁷ See *Children's Right to Privacy in the Digital Age Must Be Improved*, UNITED NATIONS HUM. RTS. OFF. OF THE HIGH COMM'R (July 15, 2021),

premise of a parent's right to care, custody, and control.⁵⁸ Additionally, it is difficult to assign responsibility regarding a child's ability to read the terms and conditions when signing up for new social media applications that subject them to the collection of personal data.⁵⁹ This issue presents another question: what makes a thirteen-year-old more "qualified" to accept the consequences of signing up for a social media platform, such as Facebook, as opposed to a twelve-year-old who is not allowed to create an account on the site? Additionally, the rise of the new social media application, "TikTok," has posed emerging issues regarding children due to the "For You Page" algorithm.⁶⁰ Finally, while some digital privacy initiatives have been created, a better solution is needed to further protect children, specifically from online personal data collection threats.

A. Children's Lack of Right to Privacy Under Parents' Right to Care, Custody, and Control

Children lack a right to privacy and use under parents' right to control "in the companionship, care, custody, and management"⁶¹ of their children, as "the child is not the mere creature of the State; those who nurture him and direct his destiny have the right, coupled with the high duty, to recognize and prepare him for additional obligations."⁶² This legal issue presents a difficult challenge when it comes to protecting children from technology's harms.⁶³ A parent's right to care, custody, and control has a profound hold on children's actions:

<https://www.ohchr.org/en/stories/2021/07/childrens-right-privacy-digital-age-must-be-improved>.

⁵⁸ See *Pierce v. Society of Sisters*, 268 U.S. 510, 535 (1925); see also *Troxel v. Granville*, 530 U.S. 57, 66 (2000); see also *Washington v. Glucksberg*, 521 U.S. 702 (1997).

⁵⁹ See The Children's Online Privacy Protection Act, 15 U.S.C.S. §§ 6501–6506 (LexisNexis 2000).

⁶⁰ See PATRICIA MOLONEY FIGLIOLA, CONG. RSCH. SERV., R46543, TIKTOK: TECHNOLOGY OVERVIEW AND ISSUES 2 (2020).

⁶¹ *Troxel*, 530 U.S. at 66.

⁶² *Pierce*, 268 U.S. at 535 (holding the State's law that required children to attend public schools through the age of sixteen as unconstitutional under parents' right to care, custody, and control over their children).

⁶³ See *Complying With COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (last visited May 6, 2022).

Fewer rights are more sacred than those which derive from the parent-child relationship. A society which arrogates to itself the power to intervene and disrupt that relationship can do so only for the most compelling reasons necessary to correct or protect a child from circumstances which directly threaten or affect the minor's physical or emotional health. The State and its agencies are not in the business of determining or otherwise interfering with the parent-child relationship on any less substantial grounds.⁶⁴

Under the Due Process Clause of the Fourteenth Amendment of the United States Constitution, parents have the fundamental right to direct the care, upbringing, and education of their children.⁶⁵ A parent solely retains the right to care for their child and is free of State intrusion

[S]o long as a parent adequately cares for his or her children (*i.e.*, is fit), there will normally be no reason for the State to inject itself into the private realm of the family to further question the ability of the parent to make the best decisions concerning the rearing of that parent's child.⁶⁶

In the United States, COPPA designates control to parents over what information websites can collect from their children.⁶⁷ The FTC states that COPPA imposes certain requirements on “operators of commercial websites and online services directed to children under [thirteen] that collect, use, or disclose personal information from children. It also applies to operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under [thirteen].”⁶⁸ However, what prevents a child from going against their parents' wishes and establishing an account on their own? This leads to an issue of a child accepting terms and conditions of specific platforms, regardless of if they are “of age” or not to consent to such conditions.⁶⁹ Should companies that collect personal data always be assumed to have actual knowledge that children under the age of thirteen are using their

⁶⁴ *Daber v. Div. of Child Protective Servs.*, 470 A.2d 723, 726 (Del. 1983).

⁶⁵ *Washington v. Glucksberg*, 521 U.S. 702 (1997).

⁶⁶ *Troxel*, 530 U.S. at 68-69.

⁶⁷ See The Children's Online Privacy Protection Act, 15 U.S.C.S. §§ 6501–6506 (LexisNexis 2000).

⁶⁸ See *Complying With COPPA: Frequently Asked Questions*, *supra* note 63.

⁶⁹ *Id.*

platforms and agreeing to the terms and conditions even though they lack “capacity” or “maturity” to do so?

B. Duty to Read Rule

One of the main flaws of COPPA is that the Act only applies to children under the age of thirteen.⁷⁰ “[C]ongress determined to apply the statute’s protections only to children under [thirteen], recognizing that younger children are particularly vulnerable to overreaching by marketers and may not understand the safety and privacy issues created by the online collection of personal information.”⁷¹ This leaves teens aged thirteen to seventeen with no protections under COPPA and assumes that they hold the required capacity to fully read and agree to the terms and conditions set forth on social media platforms.⁷² There are implications that children do not realistically read the terms and conditions before signing up for a social media platform, account, etc.⁷³ There are no realistic safeguards online to prevent children under the age of thirteen from lying about their birthday to create an online account.⁷⁴

For example, the first section in TikTok’s terms of service states:

The Terms form a legally binding agreement between you and us. Please take the time to read them carefully. If you are under age 18, you may only use the Services with the consent of your parent or legal guardian. Please be sure your parent or legal guardian has reviewed and discussed these Terms with you.⁷⁵

The issue is that TikTok places the burden on the child to seek out their parent’s permission and authority to review the terms of service with them. This is not a realistic expectation, as most children do not even read into the *first* section of a terms and conditions agreement.⁷⁶

⁷⁰ The Children’s Online Privacy Protection Act, 15 U.S.C.S. § 6501(1) (LexisNexis 2000).

⁷¹ See *Complying With COPPA: Frequently Asked Questions*, *supra* note 63.

⁷² See § 6501(1).

⁷³ *Id.*

⁷⁴ Allen St. John, *TikTok Violates Children’s Privacy Law, Advocates Say*, CONSUMER REPORTS (May 14, 2020), <https://www.consumerreports.org/privacy/tiktok-violates-childrens-privacy-law-advocates-say-a1025673250/>.

⁷⁵ *Terms of Service*, TIKTOK, <https://www.tiktok.com/legal/terms-of-service?lang=en#terms-us> (last visited May 6, 2022).

⁷⁶ See Jessica Guynn, *What You Need to Know Before Clicking ‘I Agree’ on That Terms of Service Agreement or Privacy Policy*, USA TODAY (Jan. 28, 2020), <https://www.usatoday.com/story/tech/2020/01/28/not-reading-the-small-print-is->

They are essentially agreeing to the terms of service between themselves and TikTok by proceeding to use the app, however, their parents have never given adequate consent to them, if under the age of maturity as defined by the terms and conditions.⁷⁷ Another issue is that COPPA pertains to those under the age of thirteen⁷⁸, however TikTok's terms and conditions state "under age [eighteen], you may only use the Services with the consent of your parent or legal guardian."⁷⁹ Thus, children are exposed to copious amounts of personal data collection and exposure because of their use of the app. The next section discusses TikTok's data collection process and the concern it poses for children.

C. Rise of TikTok and the Concerning "For You Page" Data Collection Algorithm

During the COVID-19 pandemic, children flooded app stores by downloading a social media platform that gave a sense of community during a time of social distancing and uncertainty.⁸⁰ TikTok has become a popular video app for children because its curated "For You Page" and its ability to transform ordinary children into celebrities with millions of followers.⁸¹ The app, however, has been a controversial subject regarding privacy violations and substantial data collection.⁸² Advocacy groups filed complaints with the FTC regarding TikTok's failure to destroy information collected about children under the age of thirteen.⁸³ The claim stemmed from a violation of a February 2019 FTC agreement and subjected TikTok to a fine equivalent to more than five million dollars.⁸⁴ Is a monetary fine a truly effective deterrent in the scheme of social

privacy-policy-fail/4565274002/ ("A Deloitte survey of 2,000 U.S. consumers in 2017 found that 91% of people consent to terms of service without reading them. For younger people, ages 18-34, that rate was even higher: 97% did so.").

⁷⁷ *Terms of Service*, TIKTOK, <https://www.tiktok.com/legal/terms-of-service?lang=en#terms-us> (last visited May 6, 2022).

⁷⁸ The Children's Online Privacy Protection Act, 15 U.S.C.S. § 6501(1) (LexisNexis 2000).

⁷⁹ *Terms of Service*, TIKTOK, <https://www.tiktok.com/legal/terms-of-service?lang=en#terms-us> (last visited May 6, 2022).

⁸⁰ Cynthia Littleton, *Why TikTok's Popularity Exploded During the Pandemic*, VARIETY (Jan. 27, 2021), <https://variety.com/2021/digital/news/tiktok-popularity-covid-1234893740/>.

⁸¹ St. John, *supra* note 74.

⁸² *Id.*

⁸³ *Id.*

⁸⁴ *Id.*

media platforms, such as TikTok, and other large companies that rely on personal data to maximize business? In the eyes of such companies, a five million dollar fine could be viewed as merely the cost of doing business to gain valuable information about their customers.⁸⁵

TikTok's data algorithm broadcasts videos onto the "For You Page" of other users.⁸⁶ The "For You Page" uses "artificial intelligence (AI) technologies and data mining practices."⁸⁷ In addition, Tik Tok states that "the recommendation engine relies on a complex set of weighted factors to recommend content, including hashtags and videos watched previously, as well as the kind of device a person is using."⁸⁸ TikTok's extensive data collection used to curate the "For You Page" is unsettling when being used for children. Equally problematic is the app's ability to expose children to millions of followers without parental knowledge and/or consent. Although TikTok has made reforms to its accounts for users under the age of thirteen, a child is incentivized to lie about their birthday to be in the "public eye" without parental consent.⁸⁹ TikTok uses and collects "location data and internet address, keystroke patterns, and the type of device being used to access the app."⁹⁰ It also "stores a user's browsing and search history within the app, as well as the content of any messages exchanged using the app."⁹¹ There is also additional information that can be collected based on preferences, such as "phone number, phone book, and social-network contacts; GPS data; user age; user-generated content . . . videos 'liked,' shared, watched all the way through, and re-watched."⁹² TikTok's ability to track user behavior is extremely troubling in the context of children's privacy rights, as children do not understand the extent their information is being collected.

The United States government has raised concerns with TikTok's reputation for data collection.⁹³

On August 6, 2020, President Trump signed an Executive Order aimed at stopping TikTok from doing business in the United States. If the order had gone into effect on September 27, 2020,

⁸⁵ See Franzak, *supra* note 1.

⁸⁶ FIGLIOLA, *supra* note 60.

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ St. John, *supra* note 74.

⁹⁰ *Id.*

⁹¹ *Id.*

⁹² *Id.*

⁹³ *Id.*

as scheduled, it would have prohibited any U.S. company or person from "transacting" with ByteDance. On August 14, 2020, the President issued a second Executive Order stating that ByteDance must divest from all assets that support TikTok's U.S. operations and destroy all previously collected U.S. user data. Divestiture may be accomplished by finding a U.S. buyer for TikTok. The requirements are designed to limit the Chinese government's access to current and future data from U.S. TikTok users. ByteDance does not want to divest from TikTok and sued the Trump Administration.⁹⁴

However, ByteDance reached an agreement where Oracle would become the company's technology provider.⁹⁵ Although this governmental feat was unsuccessful, this action demonstrates the magnitude of data collection through social media— these issues have caught the attention of the American government.

The social media platform, TikTok, has been of primary concern for children's privacy rights, including ordinary users and "TikTok famous" children.⁹⁶ TikTok's history, the app's rise in popularity, its data collection algorithm, the app's legal controversies involving children's privacy rights, have led to the dire need for a solution to better protect children using TikTok.⁹⁷ The FTC's fines to TikTok in violation of the FTC's consent decree are not enough to deter this behavior of heavy data collection on its child users and new regulations must be developed.⁹⁸ In addition, the FTC must act on these complaints from advocacy groups, as opposed to inaction, as COPPA is essentially meaningless without enforcement.⁹⁹ While children should have a right to use and expression on TikTok and other social media services, it is imperative to balance privacy concerns with freedom of use, as technology usage has become so integral in the current generation.¹⁰⁰

⁹⁴ *Id.*

⁹⁵ Allen St. John, *TikTok Violates Children's Privacy Law, Advocates Say*, CONSUMER REPORTS (May 14, 2020), <https://www.consumerreports.org/privacy/tiktok-violates-childrens-privacy-law-advocates-say-a1025673250/>.

⁹⁶ *Id.*

⁹⁷ FIGLIOLA, *supra* note 60.

⁹⁸ *See* St. John, *supra* note 74.

⁹⁹ *See* H.R. 44/25 Gen. Assemb., Reg. Sess. (Ga. 1990); *see also*, The Children's Online Privacy Protection Act, 15 U.S.C.S. §§ 6501–6506 (LexisNexis 2000).

¹⁰⁰ *See Children's Right to Privacy in the Digital Age Must be Improved*, *supra* note 57.

D. Current Digital Privacy Initiatives

Digital marketing is rapidly evolving, but regulating it is developing at a slower pace.¹⁰¹ Many digital privacy initiatives have been developed throughout this technological evolution, in order to better protect consumers and their information from intrusive collection by companies.¹⁰² For example, the FTC created a watchdog approach, while also promoting a self-regulation method in order to protect consumers from spying.¹⁰³ Their industry guidelines include notice, choice, access, security, and redress.¹⁰⁴

Other initiatives include the National Association of Criminal Defense Lawyers Fourth Amendment Center.¹⁰⁵ This center focuses on providing three resources.¹⁰⁶ They provide education on issues regarding technology, privacy, and constitutional rights.¹⁰⁷ They also provide resources that help lawyers in challenging government surveillance.¹⁰⁸ Finally, they also provide a legal support network to aid in current cases where technologies have infringed on the protections under the Fourth Amendment.¹⁰⁹ The purpose of this center is to combat emerging issues resulting from intrusive data collection through technology in order to protect consumers.¹¹⁰

E. Implications for Market Research Practices

The main privacy concern for consumers is the feeling of an invasion of privacy.¹¹¹ Consumers, including the parents of child consumers, want to know if their personal information is being collected, why it is collected, and to have a say in whether it is collected at all.¹¹² In the beginning of early digital marketing, several problems arose between consumers and companies.¹¹³ Online issues are that consumers were not

¹⁰¹ Kerry, *supra* note 53.

¹⁰² See Franzak, *supra* note 1, at 639.

¹⁰³ *Id.*

¹⁰⁴ *Id.*

¹⁰⁵ See *Nation's Criminal Defense Bar Launches Initiative to Educate, Litigate Privacy Challenges in a Digital Age*, *supra* note 34.

¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

¹⁰⁸ *Id.*

¹⁰⁹ *Id.*

¹¹⁰ *Id.*

¹¹¹ See Franzak, *supra* note 1, at 630.

¹¹² *Id.*

¹¹³ *Id.*

familiar with the company online, their product, or the truth to their marketing.¹¹⁴ Without a sense of trust or familiarity, consumers would not purchase online.¹¹⁵ As technology has evolved and become a key component to everyday life, consumers are becoming more receptive to digital marketing, as online marketing optimizes the customer's brand experience and builds trust to improve customer relationships.¹¹⁶

Today's culture focuses on a personalized experience between person and technology.¹¹⁷ Customers expect personalization, as 66% of consumers are more likely to use a brand that feels more like a person.¹¹⁸ Personalized experiences stem from the collection of personal information in order to develop a customer profile that focuses on their preferences.¹¹⁹ This comes with guidelines, however, that companies must adhere to in order to uphold a balance of consumer trust and personalization.¹²⁰ Use of relationship marketing to personalize an experience for customers requires companies to disclose when they obtain information, why they are doing so, and then ultimately give the consumer a choice to consent.¹²¹

For example, in the past, cookies have been a security problem with internet users.¹²² Cookies track website visitations and identify users, with the benefit of providing browsing speed.¹²³ It is through this method that companies track visitations to provide personalized experiences on other sites, based on the visitations the cookie tracked.¹²⁴ Users were not aware of the cookie being used for this purpose and felt like they were being watched.¹²⁵ Now, sites inform the user of the cookie, identify the purpose, ensure the information will be kept confidential, and offer users

¹¹⁴ *Id.*

¹¹⁵ *Id.*

¹¹⁶ *Why Does Digital Marketing Improve Customer Relationships?*, DIGIT. SCH. OF MKG. (Mar. 1, 2019), <https://digitalschoolofmarketing.co.za/blog/why-does-digital-marketing-improve-customer-relationships/>.

¹¹⁷ Erik Folgate, *Personalization Will Dominate Digital Marketing Trends in 2018*, MEDIUM BLOG (Jan. 11, 2018), <https://medium.com/@erikfolgate/personalization-will-dominate-digital-marketing-trends-in-2018-600d8376098d>.

¹¹⁸ *Id.*

¹¹⁹ *Id.*

¹²⁰ *Id.*

¹²¹ *Id.*

¹²² Franzak, *supra* note 1, at 639.

¹²³ *Id.*

¹²⁴ *Id.*

¹²⁵ *Id.*

an opportunity to disable the cookie on the site.¹²⁶ Since users are aware of what cookies are and have been given the proper information and options, they are no longer fearful of them.¹²⁷ This same concept can be adapted to market researchers who are collecting personal data through technology: meaning consumers could likely be more accepting of digital marketing if the company discloses their intentions and offers a choice to the consumer.

SOLUTIONS

A. The United Nations Convention on the Rights of a Child

The first solution to combat the battle against market research practices and protect children on social media is for the United States to adopt the UNCRC proposition. The UNCRC policy considerations state that "the child, by reason of his physical and mental immaturity, needs special safeguards and care, including appropriate legal protection, before as well as after birth."¹²⁸ Under Article 1, a "child" is considered to be under the age of eighteen.¹²⁹ If the United States adopted UNCRC, this definition of "child" would close the gap that exists through enforcement of COPPA, which does not protect teens ages thirteen to seventeen.¹³⁰

Article 13 of the UNCRC states:

1. The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.
2. The exercise of this right may be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; or (b) For the protection of national security or of public order (order public), or of public health or morals.¹³¹

¹²⁶ *Id.*

¹²⁷ *Id.*

¹²⁸ See H.R. 44/25 Gen. Assemb., Reg. Sess. (Ga. 1990).

¹²⁹ *Id.*

¹³⁰ See The Children's Online Privacy Protection Act, 15 U.S.C.S. § 6501(1) (LexisNexis 2000).

¹³¹ See H.R. 44/25 Gen. Assemb., Reg. Sess. (Ga. 1990).

Adoption of the UNCRC article 13 would allow the United States to reach a balance of protecting children from personal data intrusions, while also giving children a greater freedom of use when it comes to engaging with social media and online platforms, since their posts can be classified as “freedom of expression.” Article 14 continues this balancing policy by stating that the “parties shall respect the right of the child to freedom of thought, conscience and religion” and “parties shall respect the rights and duties of the parents and, when applicable, legal guardians, to provide direction to the child in the exercise of his or her right in a manner consistent with the evolving capacities of the child.”¹³² Article 16 demonstrates the protections the UNCRC would offer as applicable to protecting children from personal data collection online: “1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her [honor] and reputation. 2. The child has the right to the protection of the law against such interference or attacks.”¹³³

Adoption of these specific sections of the UNCRC would help to alleviate the gaps that current American law—such as COPPA—leaves in regard to children ages thirteen to seventeen.¹³⁴ It also works to balance a child’s right to use of these social media platforms, which is an important consideration that aids in promoting individuality, expression, and creativity at a vulnerable stage of a child’s life.¹³⁵ In addition, the UNCRC is cognizant of the policy considerations for protecting children from personal data collection, working to achieve a well-rounded solution that adapts with social media usage and marketing research practices as technology advances.¹³⁶

B. Importance of Reforming the Children’s Online Privacy Protection Act

In the United States, COPPA designates control to parents over what information websites can collect from their children.¹³⁷ The FTC

¹³² *Id.*

¹³³ *Id.*

¹³⁴ See The Children’s Online Privacy Protection Act, 15 U.S.C.S. § 6501(1) (LexisNexis 2000).

¹³⁵ See Jaskiran Chopra, *Teens Say Social Media Give Valuable Source of Self-Expression*, THE PIONEER (Jan. 31, 2019), <https://www.dailypioneer.com/2019/state-editions/teens-say-social-media-give-valuable-source-of-self-expression.html>.

¹³⁶ H.R. 44/25 Gen. Assemb., Reg. Sess. (Ga. 1990).

¹³⁷ See § 6501–6506.

states that COPPA “imposes certain requirements on operators of websites or online services directed to children under thirteen years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under thirteen years of age.”¹³⁸ This Note proposes further regulation to work in tandem with COPPA, such as the UNCRC. COPPA has several flaws that hinder its enforcement for best protecting America’s children from companies that prey on social media users for personal data collection.

First, COPPA only applies to children under the age of thirteen: “[i]n enacting the Children’s Online Privacy Protection Act, Congress determined to apply the statute’s protections only to children under [thirteen], recognizing that younger children are particularly vulnerable to overreaching by marketers and may not understand the safety and privacy issues created by the online collection of personal information.”¹³⁹ The FTC admits the concern for teen privacy, yet only guidance exists for teens and parents, as opposed to specific regulations.¹⁴⁰ Further regulation is needed to protect teens from the vulnerable position they are in.

Second, the FTC admits on their COPPA Frequently Asked Questions page that the Act does not prevent children from lying about their age to register for accounts on various websites and social media platforms¹⁴¹:

COPPA covers operators of general audience websites or online services only where such operators have actual knowledge that a child under age [thirteen] is the person providing personal information. The Rule does not require operators to ask the age of visitors. However, an operator of a general audience site or service that chooses to screen its users for age in a neutral fashion may rely on the age information its users enter, even if that age information is not accurate. In some circumstances, this may mean that children are able to register on a site or service in violation of the operator’s Terms of Service.¹⁴²

¹³⁸ *Id.*

¹³⁹ See *Complying With COPPA: Frequently Asked Questions*, *supra* note 63.

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² *Id.*

The FTC enforces COPPA violations by making companies liable for civil penalties up to \$46,517 per violation.¹⁴³

The amount of civil penalties the FTC seeks or a court assesses may turn on a number of factors, including the egregiousness of the violations, whether the operator has previously violated the Rule, the number of children involved, the amount and type of personal information collected, how the information was used, whether it was shared with third parties, and the size of the company. The determination of the appropriate civil penalty will vary on a case-by-case basis.¹⁴⁴

Thus, COPPA should be broadened to include and protect teens, not just those under the age of thirteen, from marketing practices and personal data collection. Josh Golin, executive director of the Campaign for a Commercial Free Childhood states, “We’ve got a crisis of enforcement. Right now we are incentivizing companies to not know that children are on their sites. . . . They’ve literally been rewarded for pretending that there are no children on their sites.”¹⁴⁵ Specifically, however, there is an issue with protection and enforcement of those ages thirteen and under:

The federal government’s efforts to thwart these rising threats have been weakened by court rulings, uneven enforcement and the relentless pace of technological change. Surveys show that four out of five American preteens use some form of social media, with YouTube being the most popular but Instagram, Facebook and Snapchat also widely used — even though all four services officially prohibit users younger than [thirteen].¹⁴⁶

These methods of self-regulation mentioned by the FTC for years argued that “self-regulation” was an effective alternative to governmental regulation and enforceability.¹⁴⁷ In essence, they are a weak solution to a prevalent problem and require reform.

Additionally, the FTC should enforce violations by more than just a fine, as the lucrative nature of the personal data can be more substantial

¹⁴³ *Id.*

¹⁴⁴ *Id.*

¹⁴⁵ Craig Timberg, *Sex, Drugs, and Self-Harm: Where 20 Years of Child Online Protection Law Went Wrong*, WASH. POST (June 13, 2019), <https://www.washingtonpost.com/technology/2019/06/13/sex-drugs-self-harm-where-years-child-online-protection-law-went-wrong/>.

¹⁴⁶ *Id.*

¹⁴⁷ *Id.*

than a fine in the eyes of a company.¹⁴⁸ A main criticism of COPPA's current penalties is that "[e]ven when federal authorities take action, the penalties typically come many years after the violations began and make little dent in corporate profit margins, the advocates say."¹⁴⁹

Finally, COPPA should be paired with adoption of the UNCRC to best protect children from personal data intrusions online, as it is not effective when enforced on its own and would include "children" to mean anyone under the age of eighteen¹⁵⁰:

Other popular online offerings — such as the game Fortnite, which has proved to be so engrossing to preteen boys that parents worry about addiction — maintain they are "not directed" at children. But the services also don't ask users how old they are. This tactic, lawyers say, helps the companies sidestep the Children's Online Privacy Protection Act, a 1998 law known by the acronym COPPA that restricts the tracking and targeting of those younger than [thirteen] but requires "actual knowledge" of a user's age as a key trigger to enforcement.¹⁵¹

While COPPA does outline what can be done to better protect the current generation from personal data collection, the FTC must be called to action to impose more effective deterrents to maximize enforceability.

C. Criticism of Parental Control

Melinda A. Roberts, Assistant Professor of Philosophy at Trenton State College, raises a compelling argument as to the interests of a child against a parent's right to control:

[A]bsolutist doctrines of parental and custodial rights are sometimes used to protect the parent's interests to the exclusion of the child's [interests], in cases of conflict regarding fundamental matters. But it seems a flaw in these doctrines that the parent should *always* win. Fairness would seem rather to require that family law concern itself with the interests of each member of the family, not just the interests of adult members of the family.¹⁵²

¹⁴⁸ See Franzak, *supra* note 1; see also St. John, *supra* note 74.

¹⁴⁹ Timberg, *supra* note 145.

¹⁵⁰ H.R. 44/25 Gen. Assemb., Reg. Sess. (Ga. 1990).

¹⁵¹ *Id.*

¹⁵² Melinda A. Roberts, *Parent and Child Conflict: Between Liberty and Responsibility*, 10 Notre Dame J. L. Ethics & Pub Pol'y 485, 486 (1996).

She continues: “These children are ‘persons’ within the meaning of the Bill of Rights. We have so held over and over again... It is the [child's] judgment, not his parents', that is essential if we are to give full meaning to what we have said about the Bill of Rights.”¹⁵³ Although parents have a right to care, custody, and control over their children¹⁵⁴ and COPPA allows parents to make decisions as to their child’s online permissions when under the age of thirteen¹⁵⁵, children should be given their own right to privacy to use, to an extent, when it comes to engaging in social media and online personal data disclosures. Professor Roberts continues:

Having “constitutionalized” parental rights under the Fourteenth Amendment but left children's interests to the state's general authority to preserve the health and welfare of its citizens, we have constructed a system in which the most serious conflicts between parent and child are virtually always resolved in favor of the parent. Thus the system has effectively muted the voices of children and lent support to the fiction that children's interests must be whatever their parents' interests in fact are.¹⁵⁶

As technology and social media platforms develop, there must be a balance giving children the freedom to use technology and simultaneously maintaining public policy considerations of their protection on the internet from personal data collection for market research practices. While it is imperative to protect children from exposure of their personal details to unknown third parties, children are growing up in a technology-based society. Social media interaction on various applications is an integral part of modern-day society. Perhaps the younger children are exposed to these concepts and interactions, the more equipped they will be to protect themselves against unwanted personal data intrusions. Children should be given freedom to use these social media platforms for their own entertainment and gain without being limited by the fear of companies preying on their personal information. A balance of these freedoms is an ultimate goal to be

¹⁵³ *Id.* at 485.

¹⁵⁴ *See* *Pierce v. Society of Sisters*, 268 U.S. 510, 535 (1925); *see also* *Troxel v. Granville*, 530 U.S. 57, 66 (2000); *see also* *Washington v. Glucksberg*, 521 U.S. 702 (1997).

¹⁵⁵ *See* The Children’s Online Privacy Protection Act, 15 U.S.C.S. § 6501(1) (LexisNexis 2000).

¹⁵⁶ Roberts, *supra* note 152, at 488-90.

reached throughout the development of technology and social media platforms with marketing research.

CONCLUSION

The rise of technology and social media in the field of marketing research has implicated several legal issues as to consumer privacy rights, especially for those of children. While today's generation has been grandfathered into the technological world, with its use as an integral part of their childhood, parents do have a right to protect their children from the personal data intrusions that stem from marketing research on these social platforms. Parents have a right to care, custody, and control of their children, however children should also be allowed a balance of freedom to use and privacy on these social platforms. Additionally, COPPA does protect children under the age of thirteen, and gives parents some say as to their online behavior from websites that collect personal data. However, there are no protections under COPPA for teens that are being subjected to personal data collection through marketing research practices on these social applications. The ages of thirteen to seventeen are left in a vulnerable state.

Additionally, the FTC enforces COPPA through monetary fines to data mining companies, however, the fines are miniscule in comparison to how lucrative individualized data is for marketing research practices of these companies. Thus, COPPA should be reformed to include protections for teens aged thirteen to seventeen. COPPA should also be enforced in tandem with the UNCRC to best protect America's children from the intrusions of personal data collection that is promulgated through social media usage. By incorporating the UNCRC, COPPA will better deter companies from engaging in such practices, as they will not *just* be subject to a fine as a penalty. Finally, a balance should be met that allows children a larger freedom to use in terms of engaging on social media, while upholding the rooted American tradition of a parent's right to care, custody, and control over their children's online usage.