UCLA Journal
of
Law & Technology

Minors, Consent, and Facebook: Why Disaffirmance is Insufficient to Protecting Minors' Privacy on Social Media

Rachel Dow[1]

ABSTRACT

Teens increasingly live their lives online. Surveys estimate that teens spend at least four hours per day on social media and over eighty percent of teens use Instagram. As such, the ability for minors to contract with these online services raises a variety of concerns, particularly about consent. Generally, a minor can provide consent in two ways: (1) a parent or legal guardian can consent directly on their behalf; or (2) a minor can consent directly, but the contract is subject to disaffirmance. In June 2021, the California Legislature unanimously passed AB 891. The bill was a reaction to the increasing prevalence of representative consent provisions in contracts for online platforms. Online companies use such provisions in an attempt to establish that a minor's representation of their parent's consent constitutes a legally enforceable contract that is not subject to disaffirmance.

In this paper, I argue the focus on disaffirmance as the tool to protect minors contracting online is misplaced when dealing with social media. Social media presents different contexts and challenges to consent than the traditional marketplace, upon which the principal of disaffirmance was based. The focus should instead be on whether minors can consent to these platforms' terms of service at all because of the lack of transparency around the collection and commercialization of personal data, algorithms that purposefully amplify harmful content to increase engagement for purposes of increased profit, and the lack of viable alternative platforms. Instead of focusing on the decisions of minors and disaffirmance, as is the case with AB 891, we should instead emphasize approaches such as

[1] J.D. 2022, UCLA School of Law.

adopting the GDPR's definitions of consent and various avenues to hold platforms liable under tort law for harms to minors resulting from social media.

TABLE OF CONTENTS

INTRODUCTION

Social media has radically changed the way we interact with peers, friends, and family. For teens, social media has become a defining aspect of life over the past decade. In 2021, at least 81% of American teens used Instagram, 77% used Snapchat, and 73% used TikTok.[2] On average, teens reported spending at least four hours per day on social media.[3] The ability to communicate with others through social media proved particularly important during the COVID-19 lockdowns. But social media can also increase mental health problems, including anorexia and suicidal ideations, and make minors more vulnerable to actions by both predatory adults and profit-driven companies.

Recently, reporting and whistle blower testimony about how Facebook uses personal data for commercial purposes, including amplifying harmful content to increase engagement, has re-inflamed the conversation about teens, the Internet, and safety. Facebook even paused its development of Instagram Kids because of the avalanche of criticism.[4] The debate about teens' social media use has also renewed discussion of a basic component of contract law: the right of minors to disaffirm. While disaffirmance provides minors an opportunity to nullify a contract without penalty, its power is greatly weakened when applied to social media platforms and minor consent to terms of service agreements.

In this paper, I argue disaffirmance is an inadequate tool to protect minors contracting with social media entities online because social media presents a different context and challenge to consent than the traditional marketplace, upon which the principal of disaffirmance was based. The focus should instead be on whether minors can consent to these platforms' terms of service at all because of the lack of transparency around the collection and commercialization of personal data, algorithms that purposefully amplify harmful content to increase engagement to increase profit, and the lack of viable alternative platforms. Part I explains existing

---

[2] PIPER SANDLER, TAKING STOCK WITH TEENS: 21 YEARS OF RESEARCHING U.S. TEENS GENZ INSIGHTS (Fall 2021), https://piper2.bluematrix.com/docs/pdf/3bad99c6-e44a-4424-8fb1-0e3adfcbd1d4.pdf?utm_source=morning_brew&utm_medium=newsletter&utm_campaign=mb.

[3] *Id.*

[4] Adam Satariano & Ryan Mac, *Facebook Delays Instagram App for Users 13 and Younger*, N.Y. TIMES, https://www.nytimes.com/2021/09/27/technology/facebook-instagram-for-kids.html (Oct. 4, 2021).

contract and case law as it applies to minors and online activities, particularly social media. Part II lays out why disaffirmance is an inadequate protection for minors on social media. Part III offers potential solutions, including adopting the European Union's General Data Protection Regulation's ("GDPR") definitions of consent and various avenues to hold platforms liable under tort law for harms to minors resulting from social media.

I. Existing Contract Law and its Application to Minors

California Family Code section 6700 provides that "a minor[5] may make a contract in the same manner as an adult, subject to the power of disaffirmance," with three exceptions.[6] The three exceptions are contracts that: (a) delegate power; (b) relate to real property or any interest therein; or (c) relate to any personal property not in the immediate possession or control of the minor.[7]

Disaffirmance is a powerful tool. Under California law, a minor may disaffirm nearly any contract,[8] including "disaffirm[ing] all obligations . . . even for services previously rendered, without restoring consideration or the value of services rendered to the other party."[9] If a minor does disaffirm a contract, however, they "must disaffirm the entire contract, not just the irksome provisions."[10] California courts overwhelmingly support the policy behind disaffirmance because it "shields minors from their lack of judgment and experience. . . . [and is] for his protection against his own improvidence and the designs of others."[11] Strong judicial support for disaffirmance exists despite recognition of the burdens the tool places on those contracting with a minor.[12]

---

[5] California law defines a minor as a person under eighteen years of age. CAL. FAM. CODE § 6500.

[6] CAL. FAM. CODE § 6700.

[7] CAL. FAM. CODE § 6701.

[8] CAL. FAM. CODE § 6710 ("Except as otherwise provided by statute, a contract of a minor may be disaffirmed by the minor before majority or within a reasonable time afterwards or, in case of the minor's death within that period, by the minor's heirs or personal representative.").

[9] I.B. *ex rel.* Fife v. Facebook, Inc., 905 F. Supp. 2d 989, 1001 (N.D. Cal. 2012) (emphasis omitted) (quoting Deck v. Spartz, Inc., 2011 WL 7775067, at 7 (E.D. Cal. Sept. 27, 2011)).

[10] E.K.D. *ex rel.* Dawes v. Facebook, Inc., 885 F. Supp. 2d 894, 899 (S.D. Ill. 2012) (quoting Holland v. Universal Underwriters Ins. Co., 270 Cal. App. 2d 417, 421 (1969)).

[11] Berg v. Traylor, 148 Cal. App. 4th 809, 818 (2007) (quoting Niemann v. Deverich, 98 Cal. App. 2d 787, 793 (1950) (internal quotation marks omitted)).

[12] *E.g.*, *id.* ("Any loss occasioned by the disaffirmance of a minor's contract might have been avoided by declining to enter into the contract.").

As one California court stated, "[O]ne who provides a minor with goods and services does so at their own risk."[13] Thus, any party who enters into a contract with a minor must be aware that the minor is empowered to walk away from the contract at any time.

Consent further complicates the regime governing contracts with minors. A fundamental principle of contract law mandates that, when contracting, all parties provide voluntary consent. Consent is defined as an "agreement, approval, or permission as to some act or purpose, esp[ecially] given voluntarily by a competent person."[14] True consent is "an act unclouded by fraud, duress, or sometimes even mistake."[15] There are two ways to obtain consent when contracting with a minor: (1) direct consent; and (2) verifiable consent. When a minor gives direct consent, the contract is subject to disaffirmance. A party can obtain verifiable consent through the minor's parent or legal guardian on behalf of a minor. Verifiable consent must be verified through a third party (i.e., through providing a government issued I.D. or a calling system that has the parent answer multiple security questions).[16] Verified consent is not subject to disaffirmance. But some online companies have attempted to create a third form of consent: representative consent. A minor provides representative consent by representing that their parent or legal guardian has provided consent. The minor does not have to verify that the parent or legal guardian has indeed provided this consent. Below, I outline existing federal and California law governing the rights and protections of minors online including both regulatory regimes and caselaw. I then discuss the history of AB 891 and its intended purpose.

A. Minors' Contracts and Online Companies

As this paper will discuss, the assumptions, justifications, and concerns traditionally animating the right of minors to contract is complicated.[17] Before that discussion, however, it is important to understand existing federal and California law governing the rights and protections of minors online.

---

[13] *Id.* at 816 (citing Goldberg v. Superior Ct., 23 Cal. App. 4th 1378, 1382–83 (1994)).
[14] *Consent*, BLACK'S LAW DICTIONARY (9th ed. 2009).
[15] [15] *Consent*, Black's Law Dictionary (6th ed. 1994).
[16] This is the type of consent required by COPPA. *See* discussion *infra* Section I.a.i.
[17] *See* discussion *infra* Part II.

i. Overview of Existing Regulatory Regime

Both California and federal law governs the behavior and rights of minors online. In 1998, Congress passed the Children's Online Privacy Protection Act of 1998 ("COPPA").[18] COPPA applies only to minors under the age of thirteen.[19] COPPA makes it illegal for any website or other online service that collects personal information from users to collect such personal information from minors without obtaining verifiable parental consent for any collection, use, or disclosure of the minor's personal information.[20] Because obtaining verifiable consent is so burdensome for companies, many websites and nearly all social media sites, do not allow children under thirteen to use the service at all.[21]

In 2018, the California State Legislature passed the California Consumer Privacy Act ("CCPA").[22] CCPA created requirements for businesses that collect consumers' personal information including mandating that businesses disclose what information has been collected, provide notice of such collection, and allow consumers to opt out of the sale of their personal information to third parties.[23] The CCPA further restricts the sale of a consumer's personal information when that consumer is a minor.[24] Like COPPA, for minors under the age of thirteen, a business must first obtain the consent of a minor's parent or guardian.[25] For minors between the ages of thirteen and sixteen, a business must obtain direct consent from the minor for the sale of their personal information.[26] Because those thirteen to sixteen years old could provide direct consent, any contract created with these minors is subject to disaffirmance.

---

[18] 15 U.S.C. §§ 6501–6505.

[19] 15 U.S.C. § 6501(1) (defining "child" as an "individual under the age of 13."). This is different from California law, which defines a "minor" as someone under eighteen years of age, CAL. FAM. CODE § 6500, but consistent with the definition of a minor under the CCPA, CAL. CIV. CODE § 1798.120(c)–(d).

[20] 15 U.S.C. § 6502(b)(1)(A)(ii).

[21] For example, a minor must be at least thirteen years old to lawfully create both a TikTok and Facebook account.

[22] CAL. CIV. CODE §§ 1798.100–1798.199.95.

[23] CAL. CIV. CODE §§ 1798.100–1798.20.

[24] CAL. CIV. CODE § 1798.120(c) (The CCPA prohibits a business from selling the personal information of consumers if it "has actual knowledge that the consumer is less than 16 years of age" and states that "[a] business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.").

[25] *Id.* This is verified consent and therefore not subject to disaffirmance.

[26] *Id.*

ii. California Case Law

Many lawsuits brought against tech companies involving minors and consent are decided in the Northern District of California, home of Silicon Valley. These cases illustrate that no clear interpretation of California contract law, COPPA, and the CCPA has emerged.

The initial major litigation against tech companies' business practices involving minors fits within existing understandings of contracts and traditional marketplace business transactions. In *In re Apple In-App Purchase Litig.*, a class of parents brought suit against Apple alleging that their minor children were able to purchase "game currencies" for apps that were advertised as free without the parents' knowledge of authorization.[27] Although downloading the app game was free, it required Apple users to enter their password.[28] In doing so, access to the full account remained open for fifteen minutes without the need to re-enter the password.[29] Thus, for fifteen minutes, children could charge their parents' accounts without their knowledge or consent.[30] The charges on the plaintiffs' accounts ranged from $99.99 to $338.72 per fifteen-minute period.[31] In addition to other relief, the plaintiffs sought to void the purchases made by their children, alleging that each purchase was a sales contract between Apple and a minor and thus could be disaffirmed.[32] In denying Apple's motion to dismiss, the court preliminarily rejected Apple's argument that its "Terms & Conditions" constituted a contract that governed every successive transaction.[33] The case ultimately settled.

A similar story occurred in *I.B. ex rel. Fife v. Facebook, Inc.*[34] In *I.B.*, a minor unknowingly used his mother's credit card to purchase several hundred dollars of "Ninja Saga" in-game purchases believing he was only purchasing virtual currency.[35] Another minor made over $1,000 of purchases.[36] While the court rejected plaintiffs' argument that the purchases were void under Family Code section 6701(a) (delegation of power), the court found that plaintiffs had

---

[27] *In re* Apple In-App Purchase Litig., 855 F. Supp. 2d 1030, 1033 (N.D. Cal. 2012).
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] *Id.* at 1034.
[32] *Id.* at 1035.
[33] *Id.* at 1036.
[34] I.B. *ex rel.* Fife v. Facebook, Inc., 905 F. Supp. 2d 989 (N.D. Cal. 2012).
[35] *Id.* at 996.
[36] *Id.*

alleged a plausible claim that the purchases are void contracts under section 6701(c) (personal property not in immediate possession). Furthermore, the court discussed these contracts could be disaffirmed "even after receiving the benefits" of the purchases[37] and despite the fact the purchases were made with the minors' parents' credit cards.[38] The case ultimately settled.

Although not simple cases, *In re Apple* and *I.B.* both focused on the issue of direct purchases and are thus more straightforward applications of existing contract law than cases dealing with usage of consumers' personal information and advertising. *Cohen v. Facebook, Inc*. was one of the first major challenges to online companies' use of personal information. In *Cohen*, plaintiffs challenged the "Friend Finder" feature,[39] specifically alleging that Facebook "used their names and profile pictures to promote the Friend Finder without their knowledge or consent" and thus "misappropriated both their names and likeness of commercial purposes."[40] While ultimately granting Facebook's motion to dismiss, the court did leave open whether Facebook has the "unequivocal legal right to use the plaintiffs' names and profile pictures" because of users agreeing to its terms of service.[41]

That same year, plaintiffs (both adults and minors) challenged Facebook's "Sponsored Stories" in *Fraley v. Facebook*.[42] Sponsored Stories was an advertising practice in which a "friend's" name, profile picture, and assertion that the person "likes" a particular company or product would appear on a user's Facebook page.[43] Plaintiffs alleged that "Facebook unlawfully misappropriated Plaintiffs' names,

---

[37] *Id.* at 1003 ("Any unfair windfall that would be potentially gained by the minors might have been avoided by declining to enter into the contract.") (internal quotation marks and citations omitted).

[38] *Id.* at 1004.

[39] Cohen v. Facebook, Inc., 798 F. Supp. 2d 1090, 1092 (N.D. Cal. 2011) (explaining that Facebook's Friend Finder would use access to a user's email account to search for contacts that the user is not yet Facebook friends with, as well as to send emails inviting non-Facebook users from the contact list to join Facebook).

[40] *Id.*

[41] *Id.* at 1092-93.

[42] Fraley v. Facebook, Inc., 830 F. Supp. 2d 785 (N.D. Cal. 2011). Sponsored Stories was previously challenged in E.K.D. *ex rel.* Dawes v. Facebook, Inc., 885 F. Supp. 2d 894 (S.D. Ill. 2012). However, the *E.K.D.* case dealt with the issue of disaffirmance as applied for forum selection clauses. The *E.K.D.* court concluded that minors may not disaffirm Facebook's forum selection clause. *Id.* at 899 ("In the specific context of forum-selection clauses, courts . . . have readily declined to permit minors to accept the benefits of a contract, then seek to void the contract in an attempt to escape the consequences of a clause that does not suit them.").

[43] *Fraley*, 830 F. Supp. 2d at 790.

photographs, likenesses, and identifies for use in paid advertisements without obtaining Plaintiffs' consent."[44] They claimed to be entitled to compensation under California law because Sponsored Stories is "a new form of advertising" where Facebook users are "unpaid and unknowing spokespersons for various products."[45] In addition to the advertising issue, there were two other problems with Sponsored Stories. First, despite Facebook's Statement of Rights and Responsibilities ("SRR") providing users options to alter their privacy settings, users could not opt out of Sponsored Stories.[46] Second, although the SRR included a provision that a user will provide permission for Facebook to use their name and profile picture in connection with commercial content, the *Fraley* plaintiffs all joined Facebook before this term was added to the SRR and Facebook never asked users to review or re-affirm the terms before introducing Sponsored Stories.[47] The court rejected Facebook's motion to dismiss, finding that plaintiffs satisfied Article III standing,[48] immunity under § 230 was inapplicable,[49] and plaintiffs had sufficiently alleged a claim under both Civil Code § 3344 for misappropriation[50] and California's Unfair Competition Law ("UCL").[51]

---

[44] *Id.*

[45] *Id.* at 792. Notably, the court takes some time to explain both how central advertising is to Facebook's business and how the Sponsored Stories program maximizes advertising revenue. The opinion quotes Mark Zuckerberg as stating, "nothing influences people more than a recommendation from a trusted friend." *Id.* (internal notations omitted). Facebook found that members are twice as likely to remember a Sponsored Story advertisement and three times as likely to purchase the product. *Id.* By some estimates, Sponsored Stories advertisements were 46% more effective than standard advertisements. Brian Feldman, *Facebook Reaches Settlement in Sponsored Stories Lawsuit*, THE ATLANTIC (Aug. 27, 2013), https://www.theatlantic.com/technology/archive/2013/08/facebook-reaches-settlement-sponsored-stories/311753/.

[46] *Fraley*, 830 F. Supp. 2d at 792.

[47] *Id.*

[48] *Id.* at 797, 801 (finding that the plaintiffs established an invasion of a legally protected interested pursuant to Cal. Civ. Code § 3344's right of publicity).

[49] *Id.* at 801-803 (explaining that plaintiffs' allegations were "not of publishing tortious content, but rather of creating and developing commercial content that violates their statutory right of publicity.").

[50] *Id.* at 803-810.

[51] *Id.* at 810-814.

While *Fraley* ultimately settled for $20 million, a group composed of only minor plaintiffs opted out of the settlement and instead brought another lawsuit: *C.M.D. v. Facebook*.[52]

These minor plaintiffs argued that the consent provisions in Facebook's SRRs are unenforceable against the minors because they are void under Family Code section 6701(a) (delegation) or (c) (immediate possession) or, in the alternative, voidable under section 6710.[53] The court rejected both arguments. As to the section 6701 claims, the court found that granting Facebook the right to use information does not constitute a delegation for purposes of section 6701(a) and names and profile pictures cannot be "fairly characterized" as "personal property" for purposes of section 6701(c).[54]

The section 6710 claim proved more complicated. First, the court rejected the plaintiffs' claim because plaintiffs did not properly disaffirm the SRRs. The court explained that section 6710 would "almost certainly" allow plaintiffs to disaffirm.[55] But plaintiffs "never plainly expressed an intent to do so" and "continued to use their Facebook accounts long after this action was filed."[56] Second, the court questioned whether disaffirmance could "somehow retroactively vitiate the consent they had given through the SRRs at the time their names and profile pictures were used."[57] Thus, while a minor may disaffirm the continuance of a contract by expressing an intent to do so and ceasing to use the product or service, disaffirmance may not apply to actions already taken by the contracting party pursuant to the existing contract at the time of the action. As I discuss later, the issue of retroactive disaffirmance is of particular importance when considering the desire to protect minors' privacy online and whether minors indeed understand the terms of SRRs when providing consent in the first instance.

---

[52] C.M.D. v. Facebook, Inc., No. C 12-1216 RS, 2014 WL 1266291, at *1 (N.D. Cal. Mar. 26, 2014), aff'd sub nom. C.M.D. ex rel De Young v. Facebook Inc., 621 F. App'x 488 (9th Cir. 2015).
[53] *Id.* at 3.
[54] *Id.* at 4.
[55] *Id.*
[56] *Id.*
[57] *Id.*

B. AB 891

In June 2021, Governor Newsom signed AB 891.[58] The law is one sentence: "A representation by a minor that the minor's parent or legal guardian has consented shall not be considered consent for purposes of this chapter."[59] AB 891 appeared to be a reaction to the uncertainty regarding disaffirmance and representative consent highlighted by *Fraley* and *CMD*.[60] The legislative history of AB 891 reveals that California lawmakers three main concerns were: (1) the "arguable loophole in the law of contracts" created by representative consent;[61] (2) parental involvement in children's online lives;[62] and (3) the vulnerability of minors online.[63] Notably, the legislative history reveals that the legislature was not only concerned with tech platforms using a representative consent as a vehicle to circumvent disaffirmance, but also that the legislature possesses a general dislike of disaffirmance. "Persons who want to provide services to minors therefore, *sensibly*, contract with their adult parents or legal guardians, who have no such right of disaffirmance."[64]

The year before AB 891, the legislature passed AB 1138, which sought to require verified consent for all children under the age of thirteen.[65] Governor Newsom vetoed the bill because it overlapped extensively with COPPA and existing California law.[66] AB 891 is both more expansive and more limited than AB 1138. It is more expansive because it applies to all minors under the age of eighteen, not just those under thirteen. It is more limited in that, by its text, it deals only with representative consent as opposed to a verified consent regime. Perhaps the motivation behind AB 891 was not only to close the representative consent loophole, but also to push

[58] Assemb. B. 891, 2020-2021 Leg. Reg. Sess. (Cal. 2021); codified at Cal. Civ. Code § 1568.5. Assemb. B. 891 passed the California Legislature unanimously.

[59] *Id.*

[60] *See* Assemb. B. 891, Assemb. Comm. Jud. Analysis, at 4 (Cal. 2021) (discussing *Fraley* and examples of social media sites that continue to use representative consent in their terms of service).

[61] *Id.* at 1.

[62] *Id.* at 2 (explaining that AB 891 seeks to "ensur[e] that these parents meaningfully consent to these [online] activities – just as if they were being asked to consent to their child going on a school trip").

[63] *Id.* at 1 ("Children lack the judgment and experience to understand the potential long-term consequences of these contracts."); *see also id.* at 2 (explaining that minors are "targets for on-line marketing" as well as are "unwittingly lured into becoming marketers themselves.").

[64] *Id.* at 1 (emphasis added).

[65] Assemb. B. 1138, 2020-2021 Leg. (Cal. 2020) (vetoed by Governor Sept. 29, 2020).

[66] *Id.*

companies towards requiring verified consent, knowing that Governor Newsom would likely veto a bill requiring verified consent.

Both AB 1138 and AB 891 make plain the growing problem of trying to simultaneously protect both minors and businesses in the online world. More importantly, however, they illustrate the focus on disaffirmance as the central tool with which to protect minors online.

II. Disaffirmance's Incompatibility with Social Media Platforms

The focus on disaffirmance as the tool to protect minors online is misplaced when regulating social media. The principles underlying disaffirmance stem from the belief that minors are not sophisticated actors and cannot always appreciate the ramifications of their actions. Therefore, disaffirmance is necessary to protect minors from both their own naivety and predatory adults. But the online world, particularly social media, presents a new context. For example, the concerns surrounding minor consent and social media involve social media companies' business practices rather than decision making by a minor. Social media companies' profit generating practices, including selling personal information and targeting users with harmful content, call into question whether any user (minor or adult) can lawfully provide consent. Further, in the online space, minors are not per se unsophisticated parties. Rather, because minors spend an enormous amount of time online and social media is now central to adolescent life, minors are often more adept at using social media platforms than their parents.[67] Some argue that because minors are so comfortable using these platforms, disaffirmance should not apply to minors

[67] Pre-pandemic, the average teen spent approximately seven hours online per day. Megan Collins, *Kids are Spending More of their Lives Online. Teachers Can Help Them Understand Why.*, EDSURGE, 1 (Sept. 23, 2020), https://www.edsurge.com/news/2020-09-23-kids-are-spending-more-of-their-lives-online-teachers-can-help-them-understand-why. As a result of the COVID-19 pandemic, students spent an additional five to six hours online. *Id.* Much of this time online is spent on social media. *See* COMMON SENSE MEDIA, *The Common Sense Census: Media Use by Tweens and Teens*, 33-34 (2021), https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf. In addition, as of 2018, 95% of teens reported having a smartphone or at least access to one. Monica Anderson & Jingjing Jiang, *Teens, Social Media and Teens*, PEW RESEARCH CENTER (May 31, 2018), https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/.

entering into contracts with these online platforms.[68] But just because minors are more comfortable with the use of a social media platform does not mean that they are sophisticated parties and that legal protections afforded through disaffirmance are obsolete.[69]

There are four main aspects of social media that frustrate traditional notions of consent and therefore challenge the sufficiency of disaffirmance. These are: (1) platforms' reliance on the commercialization of users' personal information; (2) a minor who disaffirms cannot protect their personal information that has already been sold; (3) social media companies, specifically Facebook,[70] knowingly target users with harmful content to generate more revenue; and (4) social media companies do not provide enough information for users regarding the use of their data and the algorithm for users to lawfully consent to the terms of service. Below I outline how each frustrates disaffirmance as a protection mechanism for minors using Facebook[71] as an example.

A. Commercialization of Users' Personal Information

Through promoting (mostly targeted)[72] advertisements on its platforms, Facebook generates massive profits.[73] In July

---

[68] *See e.g.*, James Chang & Farnaz Alemi, *Gaming the System: A Critique of Minors' Privilege to Disaffirm Online Contracts*, 2 U.C. IRVINE L. REV. 627, 629 (2012) ("Minors are increasingly exposed to the online world at earlier and earlier ages, yet the law continues to disregard their experience and preserves a relatively unqualified privilege").

[69] *See* Michelle A. Sargent, Note, *Misplaced Misrepresentations: Why Misrepresentation-of-Age Statutes Must be Reinterpreted as They Apply to Children's Online Contracts*, 112 MICH. L. REV. 301, 301 (2013) ("While children may feel comfortable navigating websites, they are psychologically predisposed to be unsophisticated and impulsive actors online.").

[70] While Facebook, Inc. changed its name to Meta during the writing of this paper, I will continue to use the name Facebook to stay consistent with the relevant reporting on this topic. *See* Mike Isaac, *Facebook Renames Itself Meta*, N.Y. TIMES (Nov. 10, 2021), https://www.nytimes.com/2021/10/28/technology/facebook-meta-name-change.html.

[71] By using the term "Facebook," I am referring to the parent company's apps including Facebook and Instagram.

[72] Louise Matsakis, *Facebook's Targeted Ads are More Complex Than It Lets On*, WIRED (Apr. 25, 2018, 4:04 PM), https://www.wired.com/story/facebooks-targeted-ads-are-more-complex-than-it-lets-on/.

[73] Alfred Ng, *What Does It Actually Mean When a Company Says, "We Do Not Sell Your Data"?*, THE MARKUP (Sept. 2, 2021, 8:00 AM), https://themarkup.org/ask-the-markup/2021/09/02/what-does-it-actually-mean-when-a-company-says-we-do-not-sell-your-data; *see also*

2021, Facebook's advertising revenue was $28.6 billion.[74] As part of its advertising business, Facebook not only collects personal information from its users but also collects information from non-users through non-Facebook sites and apps.[75] Until November 2021, Facebook even collected biometric facial data without users' explicit "opt-in" consent.[76] While perhaps many adults cannot appreciate the implications or potential privacy consequences of Facebook's extensive data collection, minors have even more trouble grasping the risks.

B. Problem of Already Sold Data

In addition to the concerns about data collection, problems also arise when Facebook shares this data with third parties. Once Facebook shares its user data, it loses control over what happens to that data.[77] While this lack of control has obvious privacy concerns, it also undermines the effectiveness of disaffirmance. If a minor chooses to disaffirm, they cannot remove their data from the hands of the third parties with whom Facebook shared the data. Furthermore, in *CMD*, the court doubted that disaffirmance could apply retroactively.[78] Thus, while disaffirmance could

---

Alexis C. Madrigal, *Facebook Didn't Sell Your Data; It Gave It Away*, THE ATLANTIC (Dec. 19, 2018) https://www.theatlantic.com/technology/archive/2018/12/facebooks-failures-and-also-its-problems-leaking-data/578599/ (explaining Facebook's arrangements with Amazon, Netflix, Microsoft, and others to share user data across the platforms).

[74] Mike Isaac, *Facebook's Profit Surges 101 Percent on Strong Ad Sales.*, N.Y. TIMES (July 28, 2021), https://www.nytimes.com/2021/07/28/business/facebook-q2-earnings.html.

[75] Natasha Singer, *What You Don't Know About How Facebook Uses Your Data*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html (explaining how Facebook collects information on non-users through the Facebook Pixel, proprietary computer code the company provides to third party websites and apps, which enables third parties to collect data on their customers).

[76] *Id.*; Kashmir Hill & Ryan Mac, *Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System*, N.Y. TIMES (Nov. 5, 2021), https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html.

[77] Issie Lapowsky, *In Latest Facebook Data Exposure, History Repeats Itself*, WIRED (Apr. 3, 2019, 3:20 PM), https://www.wired.com/story/facebook-apps-540-million-records/ ("[W]hen Facebook shares data with third parties, it really has no control over where that data ends up or how securely it's stored."); *id.* (discussing the Cambridge Analytica scandal).

[78] *See* C.M.D. v. Facebook, Inc., No. C 12-1216 RS, 2014 WL 1266291, at *4 (N.D. Cal. Mar. 26, 2014) (questioning whether disaffirmance could

allow a minor to stop Facebook from sharing their data in the future, it provides no protection for data they already shared.

C. Harmful Content

Social media harms minors. For example, according to Facebook's own research, 66% of teen girls and 40% of teen boys experience negative social comparison (feeling badly as a result of comparing oneself to others).[79] Furthermore, social media platforms exacerbate pre-existing mental health problems. Thirteen percent of teen girls report that Instagram made their suicidal ideations worse.[80] Not only does Facebook know that Instagram is harmful for teens, but it also has developed its algorithm to push harmful content at teens to generate more revenue for the company.[81] According to Facebook whistle blower Frances Haugen, Facebook knows its amplification algorithms "lead children from innocuous topics like health recipes . . . to anorexia promoting content over a very short period of time."[82] And the company explicitly elects for its algorithm to do so to increase profitability:

> Facebook knows their engagement based ranking . . . amplifies preferences. . . And they have literally created that experiment [of whether the algorithm can lead you to anorexia content] themselves and confirmed, yes, this happens to people. So, Facebook knows that they are leading young users to anorexia content.[83]

Such harmful content generates more revenue because "content that elicits an extreme reaction from people is more likely to get a click, a comment, or a reshare."[84] Facebook has allegedly elected to continue using its algorithm, as opposed to returning to a chronological feed, because the algorithm

---

"somehow retroactively vitiate the consent they had given through the SRRs at the time time [sic] their names and profile pictures were used").

[79] *Protecting Kids Online: Testimony from a Facebook Whistleblower*, *Hearing Before the Subcomm. On Consumer Prot., Prod. Safety, and Data Sec.*, 117th Cong. (Oct. 5, 2021) (statement of Sen. Marsha Blackburn, Ranking Member, Subcomm. On Consumer Prot., Prod. Safety, and Data Sec.).

[80] *Id.* (statement of Sen. Amy Klobuchar, Member, Subcomm. On Consumer Prot., Prod. Safety, and Data Sec.).

[81] *See, e.g., id.*

[82] *Id.*

[83] *Id.*

[84] *Id.*

creates more engagement and therefore generates more profit.[85] Furthermore, Facebook appears to target younger users with extreme content because their continued use of the platform is essential to the long term success of the company.[86] Disaffirmance provides inadequate protection against harmful content because a mere change in the contractual relationship cannot remedy the harms to minors that emanate from Facebook's bombardment of extreme content.

D. Consent

The problems identified above – commercialized personal data and harmful content – as well as Facebook's general lack of transparency, call into question the role of consent.[87] As discussed at the outset of this paper, consent is defined as an "agreement, approval, or permission as to some act or purpose, esp[ecially] given voluntarily by a competent person."[88] Giving true consent is "an act unclouded by fraud, duress, or sometimes even mistake."[89] As a general matter, it seems that many Facebook users do not know much about how Facebook functions. For example, as of 2019, 74% of Facebook users said they did not know that Facebook maintained a list of their interests and traits; 51% said they were not comfortable with Facebook compiling this information; and 27% said the listings do not very or at all accurately represent them.[90] Some might argue that a lack of understanding about how Facebook collects one's data for commercial purposes frustrates the consent that user provided when agreeing to the terms of service. That argument is far stronger when dealing with the

---

[85] *Id.* ("Facebook knows that when they pick out the content . . . we spend more time on their platform, they make more money.").

[86] *Id.* ("[T]hey understand the value of younger users for the long term success of Facebook.").

[87] *See* Lisa Eadicicco, *Why Facebook Needs Transparency to Protect Its Users – and Stay in Business*, TIME (Mar. 22, 2018, 9:31 AM), https://time.com/5210017/facebook-cambridge-analytica-transparency-users-business/ (discussing issue of transparency). Even Facebook's own Oversight Board has called for Facebook to be more transparent. *Oversight Board publishes transparency report for third quarter of 2021*, META OVERSIGHT BOARD (Dec. 2021), https://oversightboard.com/news/640697330273796-oversight-board-publishes-transparency-report-for-third-quarter-of-2021/.

[88] *Consent*, BLACK'S LAW DICTIONARY 346 (9th ed. 2009).

[89] *Consent*, BLACK'S LAW DICTIONARY 305 (6th ed. 1990).

[90] Paul Hitlin et al., *Facebook Algorithms and Personal Data*, PEW RESEARCH CENTER (Jan. 16, 2019), https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/.

commercialization of a minor's personal data as well as targeting that minor with harmful content for purposes of increased profits. It is highly doubtful that a minor voluntarily gave Facebook permission to overwhelm their feed with, for example, anorexia content. In this way, disaffirmance is inapplicable as a minor perhaps did not provide lawful consent in the first instance.

Furthermore, the argument surrounding consent is complicated by the fact that there are dominant social media companies. Notwithstanding the debates, both political and legal, about whether Facebook is a monopoly,[91] it is clear Facebook is a dominant social media company. For users to communicate with one another on social media, they all need to be using the same platform. In theory, the more users a platform has, the more its users connect and communicate. The lack of alternative social media platforms makes disaffirmance a less viable choice for minors. Because consent to data sharing is a condition of consent, minors who do not want their personal data being sold to third parties or who do not want to be overwhelmed by harmful content are left with a Hobson's choice: deal with the bad or lose the ability to communicate via social media almost entirely. Because of these ways in which social media weakens the power of disaffirmance, disaffirmance is an inadequate tool with which to protect minors on social media.

III. Potential Solutions

As the inapplicability of disaffirmance to social media makes plain, it will be difficult to find solutions that address consent and privacy concerns regarding minors while also ensuring that minors still have access to social media platforms for three reasons. First, multiple policies will likely need to be adopted to address both actions by minors, such as providing consent, as well as actions by tech companies, such as the commercialization of data and use of problematic algorithms. Second, policy proposals will need to consider how to circumvent the broad protections Section 230 affords platforms where proposals seek to change platform behavior

[91] *See, e.g.*, Russell Brandom and Makena Kelly, *FTC Says Facebook Has Been a Monopoly 'since at least 2011' in Amended Antitrust Complaint*, THE VERGE (Aug. 19, 2021, 8:57 AM), https://www.theverge.com/2021/8/19/22627032/ftc-facebook-amended-antitrust-complaint-monopoly-instagram-whatsapp; *FTC Sues Facebook for Illegal Monopolization*, FED. TRADE COMM'N (Dec. 9, 2020), https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization.

via increased liability.[92] Third, because of Section 230 protections and platforms' primary focus on profits, proposals will likely need to seek to shift norms, in addition to the law, to pose a threat to profitability without invoking Section 230 immunity.[93]

Below, I outline two proposals: (1) adopting the European Union's General Data Protection Regulation's ("GDPR") requirements for consent; and (2) various avenues for tort liability. While these proposals could apply to both minors and adults who have been in some way harmed by social media platforms, they are perhaps best suited to address the harms to minors using social media discussed above.

A. GDPR Model

To address the issues of consent and transparency, the federal or state governments could look to Europe's example. In 2016, the European Union adopted the GDPR, which took effect in 2018.[94] The GDPR is seen as "the world's strongest set of data protection rules."[95] In an effort to better protect personal data, the GDPR explicitly addresses consent.[96] First, a company must tell a user in a manner separate from a

---

[92] 47 U.S.C. § 230. Specifically, Section 230 provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider," 47 U.S.C. § 230(c)(1), and "[n]o provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability or material that the provider or users considers . . . objectionable," 47 U.S.C. § 230(c)(2). As a result, tech platforms have largely avoided liability for harmful content posted on their site. *See also* David Morar and Chris Riley, *A Guide for Conceptualizing the Debate Over Section 230*, BROOKINGS (Apr. 9, 2021), https://www.brookings.edu/techstream/a-guide-for-conceptualizing-the-debate-over-section-230/ (providing an overview of the Section 230 shortcomings and the debate over reforms).

[93] *See, e.g.*, Frank Fagan, *Systemic Social Media Regulation*, 16 DUKE L. & TECH. REV. 393, 394 (2018) ("New laws that express social values . . . raise public awareness of social problems. . . . Normative claims, embodied in new laws, can generate 'norm cascades' and 'norm bandwagons,' which quickly lead to new forms of social behavior.").

[94] Regulation 2016/679, of the European Parliament and of the Council of 27 April 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), 2016 O.J. (L. 119) 1 (EU) [hereinafter "GDPR"].

[95] Matt Burgess, *What is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED (Mar. 24, 2020, 4:30 PM), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

[96] GDPR, *supra* note 92, art. 7.

general terms of service that it intends to use that user's data.[97] Second, the user has the right to withdraw consent at any time and withdraw must be as easy as giving consent.[98] Third, a company is discouraged from making consent to the utilization of a user's data a necessary condition of the contract.[99]

The first requirement – informing users about data collection – could increase the transparency of social media companies by forcing them to be explicit about their data collection systems. But to some extent, companies like Facebook already provide users some information about how their data is collected and used.[100] Therefore, such a requirement will only increase transparency if courts require companies to share more information. In Facebook's case, this may mean forcing the company to disclose details about its algorithm and advertising systems.

The second requirement – withdrawing consent – appears to empower all users regardless of age with the power of disaffirmance. For the reasons discussed in this paper, there are numerous questions about whether such a requirement is ultimately an effective tool.

The third requirement – data as a contractual condition – seems to be the most promising requirement. Social media companies make the processing of personal data a condition of their terms of service because they rely on targeted advertising for revenue, particularly where the social media service itself is free to users. This third requirement questions whether one can freely give consent in these situations. If users cannot freely consent, it does not constitute consent as required for an enforceable contract. In the absence of an enforceable contract where a social media company had sold that user's personal data to a third party, that social media company would likely face liability. Assuming (and this is a large assumption) that courts would find a lack of consent in such a situation, the risk of liability could change the behavior of social media platforms. The third requirement could also act as mitigate harmful content because such content is

---

[97] *See id*., art.7, para. 2 ("[T]he request for consent [for the user's data] shall be presented in a manner which is clearly distinguishable from the other matters.").

[98] *Id*., art.7, para. 3.

[99] *See id*., art.7, para. 4 ("When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.").

[100] *See* Privacy Policy, META (last updated Jul. 26, 2022), https://www.facebook.com/policy.php.

targeted at particular users based off their collected personal information. Facebook might switch to a chronological feed, particularly for minors, should the financial penalties become severe enough.[101]

B. Tort Liability

Another proposal for shifting the liability landscape for social media companies to better protect minors looks at the application of tort law. Below I discuss some possible avenues in tort law for holding social media companies more accountable, particularly in their behavior towards minors, including: (1) public nuisance; (2) intentional infliction of emotional distress; and (3) products liability.

i. Public Nuisance

The Restatement (Second) of Torts defines public nuisance as: "an unreasonable interference with a right common to the general public."[102] Conduct that constitutes a public nuisance is that which "involves a significant interference with the public health, the public safety, the public peace, the public comfort, or the public convenience."[103] There have been notable attempts to use public nuisance to address societal harms including tobacco, lead paint, and guns.[104] Recently, public nuisance became a theory under which to hold companies accountable for the opioid crisis.[105]

---

[101] In addition to financial penalties from more expansive legal liability, there have also been calls to grant users the right to own and sell their own data, a move that would dramatically undermine platforms' ability to generate profits. *See, e.g.*, Hannah Klein, *Andrew Yang Wants You to Own and Sell Your Data*, SLATE (June 23, 2020, 5:30 PM), https://slate.com/technology/2020/06/yang-launches-data-dividend-project.html.

[102] RESTATEMENT (SECOND) OF TORTS § 821B(1) (AM. L INST. 1979).

[103] *Id.* at § 821B(2)(a).

[104] *See* Justine Fuga, *Trading Public Nuisance for Product Safety: Reviving the Office of Technology Assessment*, 13 DREXEL L. REV. 489, 490-492 (2021) (explaining the public nuisance arguments against tobacco, lead paint, opioids, and e-cigarettes); *See also* Jonathan Turley, *Opioids, Guns and 'Public Nuisance' Lawsuits*, WALL ST. J. (Nov. 14, 2021, 12:36 PM), https://www.wsj.com/articles/guns-public-nuisance-lawsuits-supreme-court-ruling-oklahoma-opioid-johnson-and-johnson-11636904247; Michael J. Gray, *Apply Nuisance Law to Internet Obscenity*, 6 I/S J L. & POL'Y FOR INFO. SOC'Y 317 (2010) (discussing application of nuisance to obscenity).

[105] *See, e.g.*, Jan Hoffman, *The Core Legal Strategy Against Opioid Companies May Be Faltering*, N.Y. Times (Nov. 11, 2021), https://www.nytimes.com/2021/11/11/health/opioids-lawsuits-public-nuisance.html.

The theory was that "companies created a 'public nuisance' by overplaying the benefits of the opioid products and downplaying risks."[106] But a federal court in Oklahoma and a state court in California recently rejected this theory.[107] Both courts reasoned that "if public nuisance law were stretched to cover a legal product made by a manufacturer that then passed through numerous hands and had both healthy and dangerous effects, there would be no limit on the application of the law."[108]

Like guns, tobacco, and opioids, the harms that befall minors from the use of social media constitute a public health crisis.[109] Depression in teens began to rise in 2012 when social media use became widespread.[110] In a 10-year study evaluating the impact of social media on teens, researchers found a correlation between social media use and suicide risk for teenage girls.[111] The correlation between social media and suicide is acutely worrisome given that suicide is the second-leading cause of death among teenagers in the United States.[112] Recently, the Surgeon General declared youth mental health a public health crisis.[113]

---

[106] *Id*.

[107] State *ex rel*. Hunter *v. Johnson & Johnson*, 499 P.3d 719 (Okla. 2021); State v. Purdue Pharma L.P., No. 30-2014-00725287-CU-BT-CXC (Cal. Super. Ct. filed Nov. 1, 2021), available at https://www.law360.com/articles/1390531/attachments/0. *But see* San Francisco v. Purdue Pharma L.P., No. 18-cv-07591-CRB, 2022 WL 3224463 (N.D. Cal. Aug. 10, 2022) (finding that Walgreens is liable for substantially contributing to public nuisance).

[108] Hoffman, *supra* note 103.

[109] Helen Lee Bouygues, *Social Media is a Public Health Crisis, Let's Treat It Like One*, U.S. NEWS & WORLD REP. (July 20, 2021, 10:40 AM), https://www.usnews.com/news/health-news/articles/2021-07-20/social-media-is-a-public-health-crisis.

[110] Jonathan Haidt & Nick Allen, *Scrutinizing the Effects of Digital Technology on Mental Health*, NATURE (Feb. 10, 2020), https://www.nature.com/articles/d41586-020-00296-x.

[111] Christie Allen, *10-Year BYU Study Shows Elevated Suicide Risk From Excess Social Media Time for Young Teen Girls*, BYU NEWS (Feb. 3, 2021), https://news.byu.edu/intellect/10-year-byu-study-shows-elevated-suicide-risk-from-excess-social-media-time-for-young-teen-girls ("Girls who used social media for at least two to three hours per day at the beginning of the study—when they were about 13 years old—and then greatly increased their use over time were at a higher clinical risk for suicide as emerging adults.").

[112] Alicia VanOrman & Beth Jarosz, *Suicide Replaces Homicide as Second-Leading Cause of Death Among U.S. Teenagers*, POPULATION REFERENCE BUREAU (June 9, 2016), https://www.prb.org/resources/suicide-replaces-homicide-as-second-leading-cause-of-death-among-u-s-teenagers/.

[113] *See* Matt Richtel, *Surgeon General Warns of Youth Mental Health Crisis*, N.Y. TIMES (Dec. 7, 2021),

The connection between various harms and social media may be too attenuated for courts to find platforms liable, as was the case for both the gun and opioid litigation. But like the tobacco litigation, advancing a public nuisance argument could potentially result in a favorable settlement for plaintiffs. Most importantly, advancing a public nuisance argument could impact the public and political discourse surrounding social media companies by shifting norms and placing social media in the societal axis of evils alongside tobacco, guns, and opioids. Even a settlement could pressure platforms to alter their algorithm (if not get rid of it all together) for minor users and therefore stop the targeting of minor users with knowingly harmful content.

ii. Products Liability

The Restatement (Third) of Torts defines products liability, stating, "one engaged in the business of selling or otherwise distributing products who sells or distributes a defective product is subject to liability for harm to persons or property caused by the defect."[114] Products liability addresses harms from product defects and misrepresentation.[115] Some argue that products liability should be applied to AI-induced harms.[116] One could similarly argue that products liability should apply to something like the Facebook algorithm. Specifically, Facebook's failure to warn about the harms that may result from proper use of the platform, particularly the mental health consequences for minors, constitutes a products liability violation. Similarly, an argument akin to strict liability arises: the public has the right to expect safe products, and social media, particularly for minors, is unreasonably dangerous. While such arguments may seem untenable, there have been recent attempts to use products liability to hold platforms accountable in situations where they would otherwise be protected by Section 230.[117]

---

https://www.nytimes.com/2021/12/07/science/pandemic-adolescents-depression-anxiety.html.

[114] RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 1 (AM. LAW INST. 1998).

[115] *See, e.g., id.* cmt. a) ("Questions of design defects and defects based on inadequate instructions or warnings arise when the specific product unit conforms to the intended design but the intended design itself, or its sale without adequate instructions or warnings, renders the product not reasonably safe.").

[116] John Villasenor, *Products Liability Law as a Way to Address AI Harms*, BROOKINGS (Oct. 31, 2019), https://www.brookings.edu/research/products-liability-law-as-a-way-to-address-ai-harms/.

[117] *See* Herrick v. Grindr LLC, 765 Fed.App'x. 586 (2d Cir. 2019) (finding tort and product liability claims fell within Section 230 immunity and

iii. Intentional Infliction of Emotional Distress

According to the Restatement (Third) of Torts, intentional infliction of emotional distress ("IIED") occurs where, "an actor who by extreme and outrageous conduct intentionally or recklessly causes severe emotional harm to another is subject to liability for that emotional harm and, if the emotional harm causes bodily harm, also for the bodily harm."[118] IIED has been applied in instances of extreme cyberbullying, such as the tragic case of Megan Meier.[119] In these cases, the particular perpetrator of the cyberbullying is held liable under IIED. Platforms, such as MySpace in the Meier case, are protected from liability by Section 230. But applying IIED to Facebook's algorithm, particularly its choice to promote harmful content to generate increased engagement, may allow a plaintiff to sidestep the Section 230 barrier. While Facebook is not the creator of the harmful content, it is not the harmful content alone that is causing the harm. Rather, it is the targeted, relentless promotion of that content based on the platform's knowledge of a user's personal information that causes the harm. Stated another way, Facebook intentionally causes emotional distress of users to make more money. While the harm that results from promoting anorexia content is more attenuated than that which results from telling a 13-year-old girl that "[t]he world would be a better place without you,"[120] that does not mean

---

dismissing claims against queer social networking app); Daniel v. Armlist LLC, 926 N.W.2d 710 (Wis. 2019) (finding Section 230 immunity applied to firearms advertisement website and dismissing claims). *See also* Carrie Goldberg, *Herrick v. Grindr: Why Section 230 of the Communications Decency Act Must be Fixed*, LAWFARE (Aug. 14, 2019, 8:00 AM), https://www.lawfareblog.com/herrick-v-grindr-why-section-230-communications-decency-act-must-be-fixed. *Cf.* Will Duffield, *Circumventing Section 230: Product Liability Lawsuits Threaten Internet Speech*, CATO INST. (Jan. 26, 2021), https://www.cato.org/policy-analysis/circumventing-section-230-product-liability-lawsuits-threaten-internet-speech#introduction.

[118] RESTATEMENT (THIRD) OF TORTS: PHYS. & EMOT. HARM §46 (Am. Law. Inst. 2012).

[119] Megan Meier, a thirteen-year-old girl, committed suicide because of cyberbullying on MySpace. *See* "Megan's Story," MEGAN MEIER FOUND., https://www.meganmeierfoundation.org/megans-story. Specifically, Meier was cyberbullied by the mother, Lori Drew, of her former friend. *Id.* A jury found Drew guilty of violating the Computer Fraud and Abuse Act but the judgment was later vacated. *See* U.S. v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

[120] MEGAN MEIER FOUND., *supra* note 117.

the promotion of such harmful content should not also qualify under IIED.[121]

CONCLUSION

Minors deserve to exist online and to do so safely. Disaffirmance, while a powerful tool in the traditional business marketplace, fails to adequately protects minors on social media. Instead of looking to disaffirmance and placing the burden on minors, policies should instead focus on the behaviors and responsibilities of platforms. Platforms should have to be more transparent about data collection and their algorithm to ensure that users provide lawful consent when signing terms of services. Furthermore, platforms should be liable for harms resulting from amplifying harmful content.

[121] In October 2022, the Supreme Court granted certiorari in *Gonzalez v. Google LLC* on the question: "Does section 230(c)(1) immunize interactive computer services when they make targeted recommendations of Information provided by another information content provider, or only limit the liability of interactive computer services when they engage in traditional editorial functions (such as deciding whether to display or withdraw) with regard to such information?" 2 F.4th 871 (9th Cir. 2021), *cert. granted* (U.S. Oct. 3, 2022) (No. 21-1333). *Gonzalez* involves the murder of a 23-year-old U.S. citizen, Nohemi Gonzalez, in an ISIS attack while she was studying abroad in Paris, France. *See* Brief for Petitioner, *Gonzalez v. Google LLC*, (No. 21-1333) at 8. Gonzalez's estate and several family members filed suit against Google alleging that, as the owner of YouTube, Google "had aided and abetted ISIS" and that YouTube "affirmatively 'recommended ISIS videos to users.'" *Id.* at 9. While the role social media plays in the proliferation of extremism falls far outside the scope of this paper, the Supreme Court's decision will likely have broad implications regarding the extent to which social media platforms can be held liable for harms to minors. Notably, many of the amicus briefs filed focus expressly on how severe harms to minors flow directly flow from the platform's algorithms and social media companies' effort to maximize profit. *See e.g.*, Brief of the Children's Advocacy Institute at the University of San Diego School of Law as Amicus Curiae In Support of Neither Party, *Gonzalez v. Google LLC*, (No. 21-1333).