


5-2024

Minor Exploitation and Regulatory Shortfalls: Safeguarding Children's Data in the Age of Modern Technology

Kaylee Lahti
klahti@unomaha.edu

Follow this and additional works at: https://digitalcommons.unomaha.edu/university_honors_program

 Part of the [Conflict of Laws Commons](#), [First Amendment Commons](#), [Intellectual Property Law Commons](#), and the [Legislation Commons](#)

Please take our feedback survey at: https://unomaha.az1.qualtrics.com/jfe/form/SV_8cchtFmpDyGfBLE

Recommended Citation

Lahti, Kaylee, "Minor Exploitation and Regulatory Shortfalls: Safeguarding Children's Data in the Age of Modern Technology" (2024). *Theses/Capstones/Creative Projects*. 291.
https://digitalcommons.unomaha.edu/university_honors_program/291

This Dissertation/Thesis is brought to you for free and open access by the University Honors Program at DigitalCommons@UNO. It has been accepted for inclusion in Theses/Capstones/Creative Projects by an authorized administrator of DigitalCommons@UNO. For more information, please contact unodigitalcommons@unomaha.edu.

**Minor Exploitation and Regulatory Shortfalls:
Safeguarding Children's Data in the Age of Modern Technology**

Kaylee Lahti

Honors Department

HNRS4980: Senior Honors Thesis

Dr. Destynie Sewell

13 May 2024

Abstract

This paper looks into the issue of minors in the era of social media and seeks to answer the question: how can regulations help to protect children's privacy in the age of social networks? To do this, this paper will start by exploring the privacy issues that have arisen amongst minors in the modern age and the lack of accountability for social networking companies. It will then look at the current regulations related to this issue and see where these regulations have fallen short. Next, possible regulatory solutions to this issue will be explored, including looking at current laws that could be applied to this sphere or creating an entirely new framework. Finally, policy recommendations and their benefits will be discussed, which are intended to alleviate this issue.

Table of Contents

I.	Introduction	4
II.	Minors in the Social Networking Era	5
	A. Data Collection	5
	B. Data Use	6
	C. Data Sharing	8
	D. Threat of Stalking	9
	E. Threat of Exploitation	10
III.	Where Current Regulations and Bills Fail	11
	A. Section 230 of the Digital Communications Act (1996)	11
	B. Children’s Online Privacy Protection Act (COPPA) (1998)	12
	C. Children and Teens’ Online Privacy Protection Act (COPPA 2.0) (2023)	15
	D. Kids Online Safety Act (KOSA) (2023)	16
IV.	Possible Solutions to this Issue	18
	A. Applying Current Child Protection Framework	18
	B. Looking to Current Proposed Tech Laws	21
	C. Regulations Outside the U.S.	21
	D. Creating a New Framework	23
	E. Recommendations Moving Forward	24
V.	Conclusion	26
VI.	Bibliography	28

I. Introduction

Social networks are more commonplace now than ever before. This phenomenon has resulted in everything from workplace communication to political and social discourse occurring online. In this age of digital connection, it is not surprising that children are attracted to these shiny new tools as well. Unfortunately, the presence of minors in online spaces also attracts danger in many forms. This can be seen not only in individual threats such as online groomers, but also through corporate practices of data collection and use. What many people do not realize, however, is that when a minor is negatively impacted as a result of a social network, there is no available means of recourse that can be taken against that company. Despite there being federal laws in place that are intended to protect the rights of children, such as the Children's Online Privacy Protection Act of 1998 (COPPA), in recent years these sorts of regulations have proven to be ineffective, as people often exploit loopholes to violate them. In seeing this, it is clear that current regulations are insufficient to protect minors from online social networks and must be replaced with new policies which provide enforceable accountability. Thus, this paper seeks to solve this issue. To do this, this paper will start by exploring the modern situation regarding the privacy issues of minors online and social media entities' lack of accountability. It will then discuss how the current regulations in this sphere fall short of addressing either of these problems. Additionally, this paper will explore the possible legal solutions to this issue, which include adapting current laws to apply to this sphere or creating entirely new controlling entities. Finally, a policy will be proposed as a solution, and its benefits will be discussed. Overall, the American people cannot continue to allow these social networking companies to take advantage of their children for profit. Change must be enacted, and the best way to make a big impact is on a regulatory level.

II. Minors in the Social Networking Era

In modern times, it seems as though almost everyone is involved in social media in some way, whether they are working towards gaining large followings on apps like TikTok, or they simply use Facebook to stay connected with family and friends. There can be no doubt that social media attracts and engages thousands of users, and children have proven to be no different. Because of how vulnerable minors are to manipulation, however, they are often far more susceptible to the common dangers of the internet than other users.

A. Data Collection

The most common online threat is the constant practice of data collection that is performed by virtually all digital entities. Despite certain regulations like COPPA supposedly providing parents the ability to control what information online platforms are able to collect from their children, the reality of the situation is a lot messier. In a study performed in 2020 by a medical journal known as JAMA pediatrics, evidence was found that applications aimed at preschool-aged children often collect personal data for profiling and marketing purposes.

Two-thirds of apps played by 124 preschool-aged children in this cohort study showed collection and sharing of persistent digital identifiers. Children who were older, had their own mobile devices, played a higher number of apps, or were from lower-education households had higher counts of data transmissions to a higher number of third-party domains, whereas only 8% of children played apps that showed zero identifier transmissions. (Zhao et al., 2020)

While this study viewed only a small number of applications, the ratios shown in this example serve as a microcosm of the larger issue. The situation only becomes more dire when one considers that these apps are aimed at preschool-aged children, who should be the most protected

by these laws. If two-thirds of these applications gather personal data to such an egregious extent, then what is to be expected of apps that teenagers frequent?

B. Data Use

Another danger stems from what these online entities do with the data once it has been collected, which is a practice referred to as ‘data use’. Many social networking platforms focus their data use on feeding demographic information to algorithms, which in turn produce targeted advertisements and content to their users. This unfortunately is true of apps that target children as well, since loopholes can be exploited to make this possible. A court case that clearly displays the actions that many children-targeting applications perform is *New Mexico ex rel. Balderas v. Tiny Lab Productions* (516 F.Supp.3d 1293 (2021)). Within this case, the state of New Mexico brought action against a mobile games application developer for violating the *Children’s Online Privacy Protection Act* (COPPA) and the *New Mexico Unfair Practices Act* (UPA). The company, known as Tiny Lab Productions, made applications that were filled with bright colors and childlike concepts, as can be seen in some of their game titles, like “Fun Kid Racing” and “Candy Land Racing”. This company also made use of various advertisement-based software development kits (SDKs) from companies like AdMob and Applovin. Resultantly, once a child downloads a Tiny Lab app onto their device, the SDKs are installed too in the form of add components. While the child plays, these SDKs collect personal information about them and track their online behavior to create a profile for targeted advertising. All of this is performed without “reasonable and meaningful notice to the parents, or verifiable parental consent” (*New Mexico Ex Rel. Balderas v. Tiny Lab Prods.*, 516 F. Supp. 3d 1293, n.d.). Additionally, this case also involves Google, as they own and operate AdMob (providing some of the SDKs) as well as Google Play, which has a program titled “Designed for Families”. This program allows app

developers to designate their games as family friendly. In order to opt into this program, however, Google must review the developer's submitted application and assure that they meet the program's requirements.

The submitted Complaint alleges that the majority of Tiny Lab Production's applications were submitted to the Designed for Families program and approved by Google. As was summarized by Casetext, "The Complaint describes Tiny Lab's apps as 'fun, free, kid-focused games' with a 'cartoonish design and subject matter,' with 'levels [] designed specifically for children' – 'toddlers,' in particular" (*New Mexico Ex Rel. Balderas v. Tiny Lab Prods.*, 516 F. Supp. 3d 1293, n.d.). In 2018, a group of security researchers at the University of California, Berkeley, contacted Google and warned that 84 apps from Tiny Lab Productions were "potentially incorrectly listed as directed to 'mixed audiences' rather than being listed, as they should have been, as 'primarily directed to children'" (*New Mexico Ex Rel. Balderas v. Tiny Lab Prods.*, 516 F. Supp. 3d 1293, n.d.). This action is harmful because, in doing this, Tiny Labs was able to bypass COPPA's requirements and perform behavioral advertising on users under 13 years old. After performing its own investigation of the app, however, Google "did not come to the same conclusion that any of these 84 Tiny Lab Productions apps were violating COPPA," and stated that it did not consider "these apps to be designed primarily for children, but for families in general" (516 F.Supp.3d 1293 (2021)). Thus, the State of New Mexico brought this matter to court and claimed that both Tiny Lab Productions and the Ad Networks had violated COPPA.

In the original hearing in 2020, the Court concluded that the Plaintiff did not plausibly allege that the ad networks had "actual knowledge" that the app was not directed at children, and thus, they could not be held liable. It was also concluded that, in order to determine whether the

ad network had “actual knowledge”, it was not necessary to determine whether the “primary target audience” was children. In the 2021 appellate hearing, Google moved for reconsideration of the 2020 Opinion. They argued that the Court was correct in their decision regarding the liability of ad networks, but that their Opinion on the relevancy of the knowledge regarding who was the “primary target audience” was incorrect. In response, the courts reconsidered the matter and concluded that the Plaintiff had adequately proven their claims and, thus, Google’s motion to dismiss the Plaintiff’s claims was denied (516 F.Supp.3d 1293 (2021)). Despite this case resulting in a settlement, it did set the precedent for parents to sue application developers on behalf of their children. Additionally, and more importantly, it showcased the kind of behavior that is common amongst companies like Tiny Labs, who are willing to exploit loopholes to make a profit, regardless of the impact their actions have on the minors that use their products.

C. Data Sharing

Unfortunately, the issues regarding the collection of children’s data do not stop at the entity that originally collected the information. This problem compounds on itself as these companies not only use the collected data for their own purposes, but they also profit further as they sell it to third parties. This practice is known as ‘data sharing’. As a result of this practice, a child’s personal information (which could include everything from their interests to their home address) can reach the hands of thousands of companies within seconds. That reach even extends to the hands of companies like data brokers, who have no qualms about selling that information to individuals with nefarious intent. In an audit of seventy-three randomly selected mobile applications that were used in 14 states across the U.S., a team analyzed the data flow between those apps and third-party vendors. This analysis found that 60% of these school applications were sending data collected from the students to a variety of third parties. The majority of those

third parties were advertising platforms, such as Google and Facebook. It was also uncovered that 18% of these applications were sending student data to third parties that were deemed to be high-risk by the Me2B Alliance; meaning that those parties are likely to continue sharing the data with other entities, which could result in the information being spread across thousands of platforms (LeVasseur et al., 2021). This audit displays the reality of these companies' regard for children. Clearly, they see minors not as vulnerable young people in need of protection, but instead as walking collections of data that can, and should, be continually sold for profit.

D. Threat of Stalking

As a result of these practices of data collection, data use, and data sharing, young users of technology are being put at risk of serious threats with very little protections. One major threat born from these practices is that of stalking. As was stated in an article from the National Network to End Domestic Violence, "... typical activities such as tweeting, updating a Facebook status, or using a phone's GPS to find local restaurants can all be misused by abusers to stalk, harass, surveil, and control victims" (*Technology-Facilitated Stalking*, 2017). Once collected, this information is often sold to data brokers, who then offer it to anyone willing to pay (Moussa & Sherman, n.d.). One of the groups most often affected by stalking is minors, since they tend to be easier to manipulate. In a fact sheet that highlighted statistics regarding stalking amongst adolescents, it was stated that, "Among youths aged 12-18 with dating experience, 48% experienced stalking at some point in their life," and "Among youths aged 16-18 who were stalked in the past 12 months: 41% were stalked using both in-person and technology-facilitated tactics, while 34% were stalked using only technology-facilitated tactics" (*Stalking Among Adolescents: Fact Sheet*, 2022). As can be seen, the practices that social networking companies engage in to turn a profit often put young people at risk in a very real way. The issues

surrounding children's data protection are not simply a matter of morality, but also a matter of life or death for many.

E. Threat of Exploitation

Another threat that often occurs is the exploitation of minors. This danger can take form in many ways. The most obvious being that of sexual exploitation from adults online. Usually, this practice involves an older figure threatening to reveal information about a minor unless they provide sexually suggestive (or even explicit) images. Statistics regarding this issue were cited by the Child Crime Prevention and Safety Center: "According to the F.B.I., over 50 percent of the victims of online sexual exploitation are between the ages of 12 and 15. An estimated 89 percent of sexual advances directed at children occur in internet chatrooms or through instant messaging" (Kraut, 2023). These startling numbers indicate just how prevalent child exploitation is digitally.

Another occurrence that is often overlooked, however, is the exploitation of children performed by their own families. In the modern era, "family vloggers" have found a profitable niche on platforms like YouTube and Instagram. This topic was discussed in a press release from Senator Steve Padilla, noting that,

Many family influencers include their young children in their content, filming intimate details of their personal lives for their audience of millions to see. The rise of so many family content creators raises concerns about child labor and financial exploitation by parents as children are filmed without their consent and without compensation. (*Senator Padilla Introduces Child Content Creator Rights Act - Legislation Preventing Financial Exploitation of Child Influencers*, 2023).

Additionally, parents sharing their children's information and image online often results in there being issues with that child's digital footprint later in life, for instance while trying to obtain a job. Overall, whether they are being exploited for sexual favors or for their free labor, all of these situations involve children being manipulated and used by adults in online spaces.

III. Where Current Regulations and Bills Fail

With how prevalent these online threats are, it is clear that the current regulations are too insufficient to truly protect children in digital spaces. In order to gain a better grasp on the situation at hand, it is important to look at current laws and discuss where they fail.

A. Section 230 of the Digital Communications Act (1996)

One principal legislation involved in this topic is *Section 230 of the Digital Communications Act of 1934* (47 U.S.C. § 230(c)(1)). This Section was enacted by Congress in 1996 in an attempt to address growing concerns regarding the liability of online providers that carry content posted by individuals outside the company. It did this by providing limited federal immunity to the parties involved in interactive computer services. As stated in the act, "No 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)). As is explained in a report from the Congressional Research Service,

The statute generally precludes providers and users from being held liable—that is, legally responsible—for information provided by another person, but does not prevent them from being held legally responsible for information that they have developed or for activities unrelated to third-party content. Courts have interpreted Section 230 to foreclose a wide variety of lawsuits and to preempt laws that would make providers and users liable for third-party content. (Brannon, 2024)

One example of how courts have interpreted this act is the immunity being extended to guarantee safe harbor for digital social media platforms. As a result, these companies are safe from lawsuits based on their decisions to either transmit or take down users' posted content (Brannon, 2024). The immunity that Section 230 has afforded social media platforms has allowed the digital landscape to thrive like never before.

While a lot of good has stemmed from this act, however, there are negative consequences as well. As was expressed in a law review from the Department of Justice,

Criminals and other wrongdoers are increasingly turning to online platforms to engage in a host of unlawful activities, including child sexual exploitation, selling illicit drugs, cyberstalking, human trafficking, and terrorism. At the same time, courts have interpreted the scope of Section 230 immunity very broadly, diverging from its original purpose.

This expansive statutory interpretation, combined with technological developments, has reduced the incentives of online platforms to address illicit activity on their services and, at the same time, left them free to moderate lawful content without transparency or accountability. (*DEPARTMENT OF JUSTICE'S REVIEW OF SECTION 230 OF THE COMMUNICATIONS DECENCY ACT OF 1996*, 2020)

While Section 230 does have its place in modern society, a case can be made that the protections it affords are far too overreaching and do more to protect online entities from accountability in general, rather than unjust lawsuits. Thus, this law has a hand in creating the current issues that revolve around the lack of children's safety online.

B. Children's Online Privacy Protection Act (COPPA) (1998)

Regarding the topic of the digital protection of children, the primary regulation relied upon is the *Children's Online Privacy Protection Act*, otherwise known as COPPA (1998) (15

U.S.C. 6501–6505). This law has been cited in countless court hearings, but as the years pass by, its effectiveness has decreased dramatically. This is in part due to the evolution of the internet’s presence in the lives of children. An article from the Washington Post clearly illustrates this change in their statement: “In 1997, just 35 percent of households had a computer. Today, 91 percent of 14-year-olds have a smartphone — giving them unfettered access to the worst of the internet...” (Roberts, 2024). Additionally, the Northwestern Journal of Law & Social Policy found that, in 2009, 93% of Americans between the ages of twelve and seventeen had access to the internet and 61% browsed the internet daily (Matecki, 2010). This dramatic rise in internet usage among children and teens creates additional opportunities for the misuse of personal information. Along with this rise in underaged users, there was also a dramatic shift in how the internet is used: evolving from being mainly a source of information to a daily pastime, largely due to the rise of social networking sites. These sites have become indescribably popular, with recent surveys showing that 71% of teenagers have a profile on at least one social media platform (Matecki, 2010). Overall, it is clear that COPPA was passed at a time in which the digital landscape looked much different than it currently does. Thus, it is no surprise that this evolution may have led to this law becoming less effective.

Another possible cause of the current ineffectiveness of COPPA is that it only applies to children under the age of 13, which leaves out an entire demographic of teens who also require and deserve safeguarding. The main reason minors need a heightened standard of protection is because they often lack the ability to critically assess what they see online and, therefore, are vulnerable to manipulation. This fact does not just stem to the age of 13, however. Teens have consistently proven to be prone to exploitation as well. Proof of this statement can be found in figures from a research report published by Ofcom.org, in which they studied how minors

interact with online landscapes, like Google. As they stated, “Despite their being distinguished by a box with the word ‘Ad’ in it, only a minority of 8-11s (28%) and 12-15s (43%) who use search engines can correctly identify sponsored links on Google as advertising, consistent with the findings from 2016” (“Children and Parents: Media Use and Attitudes Report,” 2017). Additionally, children and teens tend to be much more likely to, by default, accept advertisements as truthful, accurate, and unbiased. Moreover, they are also more likely to overshare online, as many do not understand the permanence of this action until it is too late (“Children and Parents: Media Use and Attitudes Report,” 2017). For these reasons, teens clearly are in need of further digital protections as well, and as such, COPPA’s age range should be expanded.

COPPA’s ineffectiveness also has roots in its inability to enforce the standards it sets in place. For instance, one of its rules requires websites to collect “verifiable parental consent” before allowing the collection and use of the data of anyone under the age of 12. While on the surface this requirement seems perfectly fine, the fact that the ruling only applies to people 12 and under allows websites to exploit loopholes to avoid accountability entirely. As was described in the previously mentioned article, “While in theory this strategy may sound effective, in reality it simply encourages age fraud and allows websites to bypass the burden of obtaining parental consent” (Matecki, 2010). From the current reality of online spaces, it is clear that rather than truly making efforts to abide by these age requirements, social networking companies simply implemented easy-to-deceive security questions that, in reality, do nothing. Overall, the loopholes found within COPPA’s requirements result in websites only making vague attempts to uphold protection standards, without truly taking the necessary steps to ensure that minors are actually being protected. In general, it is clear that the modern-day digital landscape hosts a

plethora of challenges that COPPA is unequipped to handle. If children are truly to be safeguarded from digital threats, they will need more than outdated laws and unenforceable standards.

C. Children and Teens’ Online Privacy Protection Act (COPPA 2.0) (2023)

Attempting to address the issues of COPPA, a bill known as *Children and Teens’ Online Privacy Protection Act* (S. 1418) was proposed in 2023. As stated in the bill itself, this proposal was intended to, “... amend the Children’s Online Privacy Protection Act of 1998 to strengthen protections relating to the online collection, use, and disclosure of personal information of children and minors, and for other purposes” (S. 1418). To accomplish this task, this bill maps out several changes, including:

- Build on COPPA by prohibiting internet companies from collecting personal information from users who are 13 to 16 years old without their consent;
- Ban targeted advertising to children and teens;
- Revise COPPA’s “actual knowledge” standard, covering platforms that are “reasonably likely to be used” by children and protecting users who are “reasonably likely to be” children or minors;
- Create an “Eraser Button” for parents and kids by requiring companies to permit users to eliminate personal information from a child or teen when technologically feasible;
- Establish a “Digital Marketing Bill of Rights for Teens” that limits the collection of personal information of teens; and
- Establish a Youth Marketing and Privacy Division at the FTC. (*Senators Markey and Cassidy Reintroduce COPPA 2.0, Bipartisan Legislation to Protect Online Privacy of Children and Teens*, 2023)

In 2023, this bill was unanimously passed by the U.S. Senate. Despite this, however, it still has yet to be voted on in the House. This is partially caused by the concerns brought up by online entities. One prominent figure being NetChoice, a tech industry trading association and lobbying company with members like Meta Platforms, X Corp., and Google. In articles published on NetChoices' own website, the company argues that, "Both KOSA and COPPA 2.0 will in practice require online services and social media companies to collect massive amounts of data on kids, increasing opportunities for their most private information to be stolen by bad actors and predators" (Chavez, 2023). Additionally, another concern brought up by NetChoice was that this bill would give the Federal Trade Commission (FTC) more authority over online free speech, which could threaten the American public's First Amendment right (Chavez, 2024). As a result of the lobbying of companies like NetChoice, the progress COPPA 2.0 has been halted.

D. Kids Online Safety Act (KOSA) (2023)

Another regulation currently being discussed is the *Kids Online Safety Act* (KOSA) (S. 1409). As was stated in an article from Brookings.edu, "KOSA is intended to create new guidance for the Federal Trade Commission (FTC) and state AGs to penalize companies that expose children to harmful content on their platforms, including those that glamorize eating disorders, suicide, and substance abuse, among other such behaviors" (Jang et al., 2023). Some of the specific requirements of this act include requiring platforms to enable the strongest privacy settings for children by default, giving parents new controls to help protect their children, and requiring third-party audits of how online platforms are addressing their risks and impacting the well-being of teens (S. 1409). Since this bill was first introduced, there has been an uproar of opposition. One company voicing its concerns was the Electronic Frontier Foundation, which stated, "Ultimately, this puts platforms that serve young people in an impossible situation:

without clear guidance regarding what sort of design or content might lead to these harms, they would likely censor any discussions that could make them liable” (Kelley, 2023). Furthermore, KOSA was also targeted by NetChoice’s lobbying of the Senate. One of its arguments being, “... KOSA strengthens the Federal Trade Commission (FTC), which has already misused its existing power for ideological aims and ignored oversight from House Republican leadership. Lawmakers should hesitate to give this FTC further power and reject granting it authority over free speech online” (Chavez, 2024).

The concerns of NetChoice, and other like-minded companies, regarding both COPPA 2.0 and KOSA, resulted in the temporary halting of these bills’ progress. That is because they called into question the constitutionality of these bills. More specifically, they were not able to survive the strict scrutiny test, as laid out in the Supreme Court Decision of *United States v. Carolene Products Co.* (304 U.S. 144 (1938)). This test has three elements that must be met before a bill can be deemed constitutional. Firstly, there must be a compelling government interest; in this case, that would be the federal government’s interest in protecting minors. Secondly, the act has to directly advance that government interest (*Strict Scrutiny*, n.d.). In the case of COPPA 2.0 and KOSA, this element was met. The last element, however, is that the law must be narrowly tailored to achieve that interest. It is this element that was cause for concern amongst many companies. They feared that these acts set far too many restrictions on the freedom of speech and gave far too much authority to entities like the FTC (*Strict Scrutiny*, n.d.). With this being the driving factor behind the delay for both these bills, it begs the question: how can minors be properly protected online, while still allowing them to exercise their First Amendment right?

When examining these bills and regulations, the reality of the legal landscape that has resulted in these current issues becomes clear. From the fact that many of these laws are outdated in the face of newly emerging threats to the balancing act that stems from protecting minors in general while still guaranteeing their First Amendment right to the freedom of speech, there is no doubt that this situation is complex. Despite the arguments of online companies, however, there must be some solution that implements protections without leading to censorship. In order to find this solution, it is helpful to take inspiration from several sources.

IV. Possible Solutions to this Issue

To formulate a viable solution that both protects minors and the First Amendment, it is helpful to look to several sources for inspiration. From extending current child-protection regulations to the digital landscape to looking at the protections implemented outside the United States, there are many sources that may prove useful in improving the current situation.

A. Applying Current Child Protection Framework

The first regulation that may serve as a remedy to this issue would be *Section 402A of the Restatement (Second) of Torts* (Am. Law Inst. 1965). This doctrine imposes liability onto the sellers of a product whose defects lead to the physical harm of a consumer. Although its focus lies in the defects of physical products, it could be extended to the intangible products that online companies offer, that being their digital platforms. If this extension were to be enacted, social media companies would be expected to exercise reasonable care in protecting children from dangerous products, or they would face liability. The elements required for the seller to face liability are stated clearly within the doctrine:

(1) One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, if

- (a) the seller is engaged in the business of selling such a product, and
- (b) it is expected to and does reach the user or consumer without substantial change in the condition in which it is sold.

(2) The rule stated in Subsection (1) applies although

- (a) the seller has exercised all possible care in the preparation and sale of his product, and
- (b) the user or consumer has not bought the product from or entered into any contractual relation with the seller. (Harchut, 1979, p. 1035)

As can be seen within this statement, regardless of the level of possible care a seller puts into preparing their product, if the product's sale results in physical harm befalling the buyer, the company can be held liable.

This idea could easily be extended to the issue of children's lack of protection while using online devices, as social networking applications are, while intangible, still a form of product that is used to gain profit. This can be seen in how social media companies make a profit off targeted advertising algorithms and the selling of collected consumer data. Additionally, the design of data collection, use, and sharing employed by online companies unarguably results in physical harm befalling their young users, as can be seen in common threats like stalking and exploitation. These design defects are then compounded by the fact these companies fail to adequately warn their consumers of the risks that come with creating social media accounts. By drawing upon the existing regulatory foundation within Section 402A of the Restatement

(Second) of Torts and applying its tenants to the digital landscape, a foundation can be built from which digital platforms could be held accountable for the dangers embedded in the products they offer to their consumers.

Another option comes in the form of revisiting Section 230 of the Digital Communications Act of 1996 and amending it to minimize the liability exceptions given to social media companies. This idea, while promising, must be thoroughly thought out before being implemented, because while the current immunities given to social networking platforms are excessive, a complete reversal of this concept would result in a host of other problems. Thus, the solution is not to completely repeal social media companies' immunity to liability, but instead to impose limits on this immunity. This concept is discussed in an article published in Fordham Law Review, which suggests revising Section 230(c)(1) to say:

No provider or user of an interactive computer service that *takes reasonable steps to prevent or address unlawful uses of its services* shall be treated as the publisher or speaker of any information provided by another information content provider *in any action arising out of the publication of content provided by that information content provider*. (Citron & Wittes, 2017, p. 419)

As can be seen, this amendment would add the stipulation that reasonable steps of prevention must have been taken for the provider to be considered exempt from being treated as the publisher of its users' posts. As a result of this change, the scope of Section 230's immunity is clarified, and social media companies are held more accountable for their responses to the actions of their users. As the article continues, "With this revision, platforms would enjoy immunity from liability if they could show that their response to unlawful uses of their services was reasonable" (Citron & Wittes, 2017, p. 419). Overall, if these changes are made, social

networking companies would no longer be virtually immune to lawsuits, and children who are negatively impacted by the actions of these companies would finally be able to seek justice.

B. Looking to Current Proposed Tech Laws

Another possible solution may come from laws related to technology that have not yet been passed. The best example of this is *California's Age-Appropriate Design Code* (Ca. Civ. Code § 1798.99.28), which was modeled after regulations in the United Kingdom. As an article from Pluribus News stated, “It places a set of requirements on certain companies whose online services and products are likely to be accessed by youth. For instance, the law requires that all privacy settings must be set to their highest level and features that could be used to profile youth online must be disabled.” As was the case with both COPPA 2.0 and KOSA, however, California’s Age-Appropriate Design Code was lobbied against by NetChoice. In this instance, NetChoice brought California’s Attorney General, Rob Bonta, to court in a case known as *NetChoice, LLC v. Bonta* (22-cv-08861-BLF (N.D. Cal. Sep. 18, 2023)). Within this case, NetChoice once again argued that this law was unconstitutional in its scope and threatened the public’s right to the First Amendment. The lawsuit resulted in the Court siding with NetChoice and granting their motion for preliminary injunction. Thus, California’s code has been blocked ever since (*California's Youth Digital Privacy Law Heads to Court*, 2023; Jiang, 2024). Despite this law’s inability to be passed, aspects of this bill may still prove useful to build upon.

C. Regulations Outside the U.S.

Looking outside the U.S. may also prove fruitful in finding inspiration for regulatory solutions for children’s data protection. One example is the *U.K.'s Age-Appropriate Design Code* (AADC) (Section 125(1)(b) of the Data Protection Act of 2018 (2020)). This code has already served as inspiration for California’s recently proposed bill of the same name, as was

mentioned previously. Its main function is to set in place 15 standards that require online services to act in the “best interests of the child”. Some of these standards include:

- Mapping what personal data you collect from UK children.
- Checking the age of the people who visit your website, download your app or play your game.
- Switching off geolocation services that track where in the world your visitors are.
- Not using nudge techniques to encourage children to provide more personal data.
- Providing a high level of privacy by default. (Section 125(1)(b) of the Data Protection Act of 2018 (2020), pp. 7-8)

The biggest difference between the two versions is that, while both require high privacy settings by default, California’s code does not provide additional guidance on how this standard could be operationalized. Additionally, the U.K. requires data protection impact assessments (DPIAs) for all instances of risk associated with a service, whereas California only requires a DPIA when confronted with risks of “material detriment” for any service, product, or feature (Altieri et al., 2022, p. 1). Because of its far-reaching scope and comprehensive instructions, U.K.’s Age-Appropriate Design Code could function as a satisfactory solution if it were to be established in the United States.

Another source of inspiration could be found in France’s *Children’s Image Rights Law* (n°2024-120), which was passed on February 19, 2024. Within this law, children’s right to control their image is extended to protect their digital privacy as well. Its main goal is to reduce the risk of sharenting online, which is a practice that involves parents or guardians sharing photos and videos of their children on social media platforms. As was explained in an article from Connect on Tech, “The Children’s Image Rights Law reminds parents that children have

the right to privacy and the right to their image, as photos and videos are personal data... Parents or guardians can exercise their children's rights on their behalf, in particular their right to deletion if photos or videos posted by them have been reused without consent" (Clerc & Leporto, 2024). The main way that this law cuts down on sharenting and parent influencers is by requiring parents to apply for permission from the labor inspectorate before uploading a video made for profit that mainly features their child's image. Along with this, children are also assured a right of access, rectification, and erasure of their online image. Resultantly, these children (and their guardians while acting on their behalf) are able to retrospectively clean up the child's digital footprint. Such easily accessible tools would be incredibly useful for the American public, as many people struggle with poor digital footprints as they age. Additionally, this law would help to deter the online exploitation of children in the form of family vlogging, which is a practice that is currently completely unregulated. Because of these impacts, this law would be incredibly useful if implemented on a federal level within the United States.

D. Creating a New Framework

The final option for a solution would be to create an entirely new framework that would deal with this issue. This framework could come in the form of a new federal commission that would oversee the digital protection of children and their data. The overall mission of this agency would be to work with both state and local governments and social networking companies to ensure that the data protection standards for underaged users are being upheld. Through this agency, programs could be established which would operate like Drivers Education courses and provide children and their parents the opportunity to learn more about the digital landscape before being allowed to access certain online sites, such as social media platforms. This way, parents who consent to their children being online are truly giving informed consent and the

children are educated on the risks of interacting online and what conduct will keep them safe. In order for this system to work, however, software must be developed that will allow the government to keep track of who is online, which would be costly.

As can be seen, there are several options available that could serve as inspiration for a regulation that would truly address the issue of the exploitation of children online. The problem, however, is that none of these options are fool proof in the protection they provide. Each one has potential pitfalls and loopholes that may amount to no progress being made. Therefore, a combination of these options may prove to be more comprehensive and effective, but it must be weighed in relation to the Constitutional Bill of Rights in order to ensure that whatever is proposed can be passed and upheld by the courts.

E. Recommendations Moving Forward

Because this legislation involves so many factors, the right approach must involve a balancing act to achieve both comprehensive protections and the bill's constitutionality. On one hand, the solution must provide protection for minors and accountability for online entities, while also not infringing upon the First Amendment rights of American citizens. Additionally, there is also the matter of technology not yet being advanced enough to allow for the self-regulation of online companies. This is seen with how current laws that require parental consent and age verification are, in reality, ineffective as users can simply lie about their age to gain access. Thus, this policy recommendation must work to tackle all these considerations while also remaining effective.

To accomplish these disparate goals, inspiration must be taken from many sources. The first issue that must be tackled is the lack of accountability amongst online social networks. In order to remedy this issue, Section 402A of the Restatement (Second) of Torts should be

extended to intangible products, which would include the digital product of social media platforms. If this action were to be implemented, social networking companies would be required to exercise reasonable care in protecting children from these dangerous toys, or risk being held liable for any physical harm befalling their users. If this obligation were to be put onto these online companies, they would finally have true incentive to set in place tools that would actually enforce the many protections that they have ignored for decades. As a result, it is very likely that software would be made that truly could enforce the age requirements of other laws. Regardless of if that event would arise, however, there is no question that the burden of children's protections should not be put on the individual families alone. As is the case with every other type of company, social networks have the responsibility to protect their users. Just like requiring child-proof caps on medicine bottles, social media companies should have a responsibility to ensure the safety of their users.

The next goal that must be addressed is the dangers that often arise from children's presence in online spaces, those being the threat of child exploitation at the hands of their own parents, and the digital footprint that results from this exploitation. These threats can best be addressed by adopting France's Children's Image Rights Law of 2024. As was stated before, this law gives children and their legal guardians the ability to retroactively fix the child's digital footprint through rectification and erasure, and it discourages sharenting and family influencers by requiring parents to gain permission from the labor inspectorate before they upload a video for profit that prominently features their child. As a result of these measures, the exploitation of children by their parents could be tempered, and children will be able to gain control of their digital footprint so that their futures are not affected.

By implementing both Section 402A of the Restatement (Second) of Torts and the Children's Image Rights Law on a federal level in the United States, many of the threats present in the current digital landscape could be greatly mitigated. From Section 402A of the Restatement (Second) of Torts, social networking companies will finally be held accountable for the practices they allow in their spaces and, with the resulting decrease of minors on social media, the threats data collection, use, and sharing, as well as the threat of stalking should be lessened. With regards to the Children's Image Rights Law, the threats of parental exploitation of children and long-lasting digital footprints should also be controlled. And finally, it is important to note that this bill would be safe from being postponed due to First Amendment infringements. This is because it does not impose any age requirements on the public and, therefore, cannot be accused of encroaching on people's freedom of speech. Thus, it would not need to pass the strict scrutiny test and it will not be in danger of the lobbying of entities like NetChoice. From these benefits, it is clear that these policy recommendations would amount to a bill that could supply comprehensive and enforceable protections while not infringing on the public's inalienable rights. While this situation is far too complex for there to be a single, fix-all solution, this bill could mark the first step towards a future in which children can count on true digital protections.

VI. Conclusion

While the prevalence of minors being taken advantage of online is a relatively new issue, it has and will only worsen as technology continues to advance. In looking at the current legal framework surrounding the issue of children online, it is clear that these regulations are insufficient to protect minors from online social networks and, thus, they must be replaced with policies that hold these entities accountable in a real and meaningful way. With better regulations in place, young internet users will be provided the security they deserve, parents will have some

peace of mind, and social networking entities will have clear expectations and finally be held accountable for the activities they allow on their platforms. As a nation, we must uphold the belief that children are our future. As such, we have a responsibility to protect them from preventable threats. The current absence of clarity as it relates to regulatory protections for children online is an issue that is long overdue. Thus, the time is now for this nation to come together to bring about regulatory change and ensure a brighter future for generations to come.

VII. Bibliography

Altieri, C., Sanchez, B., Michelakaki, C., & Thomas, P. (2022). Policy Brief: Comparing the UK and California Age-Appropriate Design Codes. *Future of Privacy Forum*.

<https://fpf.org/wp-content/uploads/2022/11/FPF-Comparative-Analysis-of-CA-UK-Codes-of-Conduct-R3.pdf>

Brannon, V. C. (2024). Section 230: An Overview. *Congressional Research Service*.

<https://crsreports.congress.gov/product/pdf/R/R46751#:~:text=Section%20230%20of%20the%20Communications,users%20of%20interactive%20computer%20services.>

California's Age-Appropriate Design Code, Ca. Civ. Code § 1798.99.28

California's youth digital privacy law heads to court. (2023, July 27). Pluribus News.

<https://advance-lexis-com.leo.lib.unomaha.edu/document/?pdmfid=1516831&crd=2a92a147-1760-4028-9b71-d4662388b0e2&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A68T5-B3K1-JCMC-W0WV-00000-00&pdcontentcomponentid=484913&pdteaserkey=sr2&pditab=allpods&ecomp=tmnyk&earg=sr2&prid=0c9f6e45-aafd-4af8-a525-74cf40a2e519>

Chavez, K. (2023, July 27). *NetChoice Asks Senate to Reject Bills That Would Harm Children's Privacy*. NetChoice. <https://netchoice.org/netchoice-asks-senate-to-reject-bills-that-would-harm-childrens-privacy/>

Chavez, K. (2024, April 17). *Protecting Privacy & Child Safety: The Risks of Congress Rushing Flawed Legislation*. NetChoice. <https://netchoice.org/protecting-privacy-child-safety-the-risks-of-congress-rushing-flawed-legislation/>

Children and Parents: Media Use and Attitudes Report. (2017). *Ofcom*.

Children and Teens' Online Privacy Protection Act of 2023, S. 1418

Children's Image Rights Law, n°2024-120

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

Citron, D. K., & Wittes, B. (2017). The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity. *Fordham Law Review*, 86(2).

<https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5435&context=flr>

Clerc, M. D. L., & Lepertois, J. (2024, March 19). *France introduces new law to enhance the protection of children's rights in France*. Connect On Tech.

<https://www.connectontech.com/france-introduces-new-law-to-enhance-the-protection-of-childrens-rights-in-france/>

DEPARTMENT OF JUSTICE'S REVIEW OF SECTION 230 OF THE COMMUNICATIONS

DECENCY ACT OF 1996. (2020, June 3). United States Department of Justice.

<https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996>

Harchut, R. F. (1979). Products Liability—Restatement (Second) of Torts—Section 402A -

Uncertain Standards of Responsibility in Design Defect Cases—After Azzarello, Will

Manufacturers be Absolutely Liable in Pennsylvania. *Villanova Law Review*, 24(5).

<https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=2249&context=vlr>

Jang, K., Pan, L., & Lee, N. T. (2023, July 14). *The fragmentation of online child safety*

regulations. Brookings. <https://www.brookings.edu/articles/patchwork-protection-of-minors/>

- Kelley, J. (2023, May 2). *The Kids Online Safety Act is Still A Huge Danger to Our Rights Online*. Electronic Frontier Foundation. <https://www.eff.org/deeplinks/2023/05/kids-online-safety-act-still-huge-danger-our-rights-online>
- Kids Online Safety Act of 2023*, S. 1409
- Kraut, M. E. (2023). *Children and Grooming/Online Predators*. Child Crime Prevention & Safety Center. <https://chilsafety.losangelescriminallawyer.pro/children-and-grooming-online-predators.html>
- LeVasseur, L., Edwards, Z., & Alexanyan, K. (2021, May 3). *School Mobile Apps Student Data Sharing Behavior*. Me2B Alliance. <https://internetsafetylabs.org/wp-content/uploads/2021/05/school-apps-data-sharing-behavior-spotlight-report-final.pdf>
- Matecki, L. A. (2010). Update: COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era. *Northwestern Journal of Law & Social Policy*, 5(2).
<https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1058&context=njls>
- Moussa, R., & Sherman, J. (n.d.). *Data Brokers, Ad-Tech, and the Civil Liberties at Stake with Justin Sherman [S4E27]*. Retrieved November 12, 2023, from <https://www.ilpfoundry.us/podcast/data-brokers-ad-tech-and-the-civil-liberties-at-stake-with-justin-sherman-s4e27/>
- NetChoice, LLC v. Bonta*. 22-cv-08861-BLF (N.D. Cal. Sep. 18, 2023)
- New Mexico ex rel. Balderas v. Tiny Lab Prods.*, 516 F. Supp. 3d 1293. (n.d.). Casetext. Retrieved March 22, 2024, from <https://casetext.com/case/new-mexico-ex-rel-balderas-v-tiny-lab-prods-2/>

New Mexico ex rel. Balderas v. Tiny Lab Productions. 516 F.Supp.3d 1293 (2021)

Restatement (Second) of Torts § 402A cmt. b (Am. Law Inst. 1965)

Roberts, K. (2024, March 14). To protect kids online today, let's rethink this 1990s law.

Washington Post.

<https://www.washingtonpost.com/opinions/2024/03/14/communications-decency-act-protect-kids-online/>

Section 230 of the Digital Communications Act of 1934, 47 U.S.C. § 230(c)(1)

Senator Padilla Introduces Child Content Creator Rights Act—Legislation Preventing Financial

Exploitation of Child Influencers. (2023, December 18). California State Senator Steve

Padilla. <https://sd18.senate.ca.gov/news/senator-padilla-introduces-child-content-creator-rights-act-legislation-preventing-financial>

Senators Markey and Cassidy Reintroduce COPPA 2.0, Bipartisan Legislation to Protect Online

Privacy of Children and Teens. (2023, May 3). U.S. Senator Ed Markey of

Massachusetts. <https://www.markey.senate.gov/news/press-releases/senators-markey-and-cassidy-reintroduce-coppa-20-bipartisan-legislation-to-protect-online-privacy-of-children-and-teens>

Sioux City & Pacific Railroad Co. v. Stout. 84 U.S. 17 Wall. 657 657 (1873)

Stalking Among Adolescents: Fact Sheet. (2022). SPARC: Stalking Prevention Awareness, and

Resource Center. <https://www.stalkingawareness.org/wp-content/uploads/2022/01/SPARC-Stalking-and-Adolescents-Fact-Sheet.pdf>

Strict scrutiny. (n.d.). Legal Information Institute. Retrieved April 23, 2024, from

https://www.law.cornell.edu/wex/strict_scrutiny

Technology-Facilitated Stalking: What You Need to Know. (2017, May 22). NNEDV: National Network to End Domestic Violence. https://nnedv.org/latest_update/technology-facilitated-stalking/

U.K.'s Age-Appropriate Design Code, Section 125(1)(b) of the Data Protection Act of 2018 (2020), c. 12

United States v. Carolene Products Co. 304 U.S. 144 (1938)

Zhao, F., Egelman, S., Weeks, H. M., Kaciroti, N., Miller, A. L., & Radesky, J. S. (2020). Data Collection Practices of Mobile Applications Played by Preschool-Aged Children. *JAMA Pediatrics*, 174(12), e203345. <https://doi.org/10.1001/jamapediatrics.2020.3345>