Protecting Children in the Frontier of Surveillance Capitalism*

By Cole F. Watson**

I. Introduction

Modernity has precipitously arrived. Consider this paragraph describing "Internet" usage in 2002:

Every day after school, millions of children come home and immediately log onto the Internet. They happily click onto the websites of all their favorite TV shows and musical groups. As they surf these sites, the familiar fill-in-the-blank questionnaires pop up on the screen and request their names, ages, genders, addresses and phone numbers. Children plug in the necessary information and continue to click away.[1]

This once-relevant documentation of children's internet usage is now antiquated—a relic of days long gone, never to return. Today, more personal data is collected from an individual's smart phone than any "familiar fill-in-the-blank questionnaire" could reasonably solicit. A wider audience is beginning to understand that personal data is constantly collected, and controlled by companies (whether to benefit the user, shape buying habits,[2] manipulate political philosophies,[3] or something in between).[4] Even though children's internet usage is vastly different than two decades ago, the privacy protections afforded to children remain unchanged.

Society sits at an unprecedented juncture of data collection and privacy rights. Millennials will be the last generation to recall a time before the internet's proliferation. The lives of today's consumers (including children) are captured, confined, and commoditized on the internet. Because of the unprecedented acceleration of the digital frontier, we may not fully understand the repercussions of this proliferation until it is too late. As the most vulnerable and impressionable population in our society, children deserve the highest levels of legal protection.

II. Reclaiming Privacy

Privacy is a long-established right.[5] However, in comparison, consumer-protection rights are relatively new. President Woodrow Wilson created the Federal Trade Commission (FTC) in 1914 to prevent unfair competition. Additional legislation broadened the FTC's regulatory power to protect the privacy rights of consumers by prohibiting deceptive practices involving consumers' personal information.[6]

a. History of COPPA

Toward the end of the twentieth century, as more children began accessing the internet, Congress enacted the Children's Online Privacy Protection Act (COPPA).[7] COPPA requires the FTC to issue and enforce regulations concerning online privacy for children under the age of thirteen. COPPA strives to provide parental control over information collected from their children online. COPPA applies to operators of commercial websites for kids and websites that have "actual knowledge" of collecting, using, or disclosing "personal information" from children under the age of thirteen. Regarding teenage users, the FTC further explains:

> In enacting [COPPA], Congress determined to apply the statute's protections only to children under 13, recognizing that younger children are particularly vulnerable to overreaching by marketers and may not understand the safety and privacy issues created by the online collection of personal information. Although COPPA does not apply to teenagers, the FTC is concerned about teen privacy and does believe that strong, more flexible, protections may be appropriate for this age group.[8]

Notably, COPPA does not apply to information collected *about* children, only *from* children.[9] Operators must post a clear privacy policy, obtain verifiable parental consent, provide parents the ability to delete their child's information, and maintain the confidentiality of collected information. COPPA does not inhibit a child's access to certain websites; a child's parent, guardian, or school is responsible for filtering internet access.

After collecting a child's personal information and using it for its intended purpose, operators must destroy the information to prevent unauthorized access. Violators of COPPA can be liable for civil penalties up to $43,280 per violation depending on "the egregiousness of the violations, whether the operator has previously violated [COPPA], the number of children involved, the amount and type of personal information collected, how the information was used, whether it was shared with third parties, and the size of the company." Foreign-based websites that collect information from children in the U.S. and U.S.-based websites that collect information from children in foreign countries must also comply with COPPA.[10]

b. Ongoing Privacy Violations

Although some Big Tech companies pay tremendous amounts of money to settle allegations with the FTC, the quasi-punishment (which these companies agree to) may not fit the alleged crime. As such, online privacy violations continually occur.

Take for example Facebook's 2019 settlement with the FTC. The FTC determined that "Facebook repeatedly used deceptive disclosures and settings to undermine users' privacy preferences" in violation of a previous FTC order.[11] Facebook failed to inform its users that third-party apps collected data from Facebook users' "friends" without receiving proper consent. In response to the allegations that Facebook violated the previous FTC privacy order, Facebook agreed to an unprecedented $5 billion settlement with the FTC. However, to not misstate the obvious, Facebook is still alive and well, with a market capitalization of over $630 billion in March of 2022.

Also in 2019, YouTube paid $170 million to the FTC after the FTC alleged that the company illegally collected personal information from children without their parents' consent.[12] Persistent identifiers ("cookies") were used to track children who viewed child-directed channels across the internet without receiving meaningful consent from parents. Much to parents' chagrin, today's children *can* aspire to become (and sometimes already are) so-called "Youtubers." Youtubers can monetize their channel by allowing YouTube to disseminate "behaviorally targeted advertisements" to their viewers.

Today, more personal data is collected from an individual's smart phone than any "familiar fill-in-the-blank questionnaire" could reasonably solicit.

According to the FTC complaint, even though YouTube manually reviewed children's content in its "YouTube Kids" application, it still collected a child's personal data to display targeted advertisements on these channels. Despite the ubiquity of its underage viewers, YouTube denied its need to comply with COPPA. The settlement also required YouTube—and Google as its parent company—to develop, implement, and maintain a system that allows channel owners to notify YouTube of any child-directed content on their channels.

Newer companies, such as TikTok, are just as likely to violate privacy protection laws as well. For example, ByteDance, Ltd., TikTok's parent company, paid $5.7 million to the FTC after the FTC alleged that the company violated COPPA.[13] Many are familiar with the trendy TikTok dances that are used in marketing campaigns and as media memes.[14] After launching in 2016, TikTok has accumulated more than 1 billion monthly active users worldwide (many of which are children, tweens, and teenagers), with an estimated value of $75 billion in March of 2022. TikTok collects a plethora of user information: location, internet address, copied clipboard content (including text, images, and video), browsing history, messages, phone and social network contacts, and even a user's "likeness."[15] A *Wall Street Journal* analysis found that TikTok also collected unique identifiers (called "media access control" (MAC) addresses) from millions of users, which allowed the application to track these users online without the user's ability to opt out.[16] Despite the fines and flagrant data collection from

children, these platforms are socially acceptable and desirable.[17]

III. Contextualizing the Diminution of Privacy within the Framework of Surveillance Capitalism

The right to privacy transforms with each generation. George Orwell's *1984* is often cited when discussing the intersection of technology and privacy rights.[18] The issue is thinking that Orwell's imagination is still a way away: in the future, close but not quite here, or otherwise confined to its pages written decades ago. In reality, "Big Tech" replaced "Big Brother" a generation ago. While older generations gradually discover their online activity is under constant surveillance, younger generations' right to online protection is vaporizing.

a. Surveillance Capitalism Defined

In her seminal work, *The Age of Surveillance Capitalism*, Professor Shoshana Zuboff defines "surveillance capitalism" as "the new logic of accumulation."[19] Professor Zuboff elaborates:

> Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data. Although some of these data are applied to product or service improvements, the rest are declared as a proprietary *behavioral surplus*, fed into advanced manufacturing processes known as 'machine intelligence,' and fabricated into *prediction products* that anticipate what you will do now, soon, and later. Finally, these prediction products are traded in a new kind of marketplace for behavioral predictions that I call *behavioral futures markets*. Surveillance capitalists have grown immensely wealthy from these trading operations, for many companies are eager to lay bets on our future behavior.[20]

Professor Zuboff provides a framework for understanding the novelty of surveillance capitalism: (i) the logic, (ii) the means of production, (iii) the products, and (iv) the marketplace. Google is considered the pioneer of surveillance capitalism and its success can be traced through the proliferation of its online-advertising business model.

i. The Logic

A basic tenant of industrial capitalism is that a company operates by receiving revenue from its customers—not by considering the rights and dignity of its raw materials. Google's discovery of "behavioral surplus" allowed it to "translate its nonmarket interactions" into "prediction products" readily available for advertisers. Prediction products are "surveillance assets" which ultimately produce "surveillance revenues" and "surveillance capital." The adage "If a service is free, then you're the product" echoes truth. "Instead, we are the *objects* from which raw materials are extracted and expropriated for Google's prediction factories. Predictions about our behavior are Google's products . . . . *We are the means to others' ends*."[21]

Whereas industrial capitalism expropriates nature's raw material (e.g., wood, stone, crude oil, etc.) and cuts, cleaves, and compounds commodities (e.g., lumber, countertops, plastics, etc.), surveillance capitalism captures human nature (e.g., patterns, behaviors, inclinations, etc.) and contrives "prediction products."

Customers are often the "users" of a company's product. For example, a customer of a tire shop is a customer of that tire shop precisely because he *uses* its tires. However, the logic of surveillance capitalism separates "user" from "customer": those who scroll are the users; the ads that are scrolled are the customers.

When a "user" scrolls her Instagram feed, she is "using" Instagram, but she is not Instagram's customer; she is not paying Instagram for the right to scroll; rather, advertisers are paying Instagram for the right to "use" *her* attention, time, and behavior. Instagram captures its users' attention, time, and behavior (i.e., the raw material defined as "behavioral surplus) and packages this "raw material" into "production products" which are then sold (as both the statistical likelihood of whether a user will click on an advertisement and the digital space on a user's Instagram feed) to the highest bidder. How does Instagram (or any other surveillance capitalist) do this? Through its means of production involving complex algorithms developed by teams of brilliant computer scientists.

ii. The Means of Production

Machine learning and artificial intelligence are the new means of production. As surveillance capitalists accumulate more data, their "machine intelligence" evolves and their algorithms and "prediction products" become more accurate.[22]

For a simplistic example, picture the last product you googled. Say you were searching for a new baseball glove for little Johnny. When you googled "baseball glove," did links to purchase dog food or a new oven show up at the top of the search results? Or did links for the stores that sell baseball gloves compete for your attention? This is a subset of Google's machine intelligence: Google "knows" that a user searching for "baseball glove" is most likely in the market to purchase one; with this "knowledge," Google runs a microsecond auction for companies (e.g., Academy, Dick's Sporting Goods, Amazon, Wilson, etc.) to bid for your attention in hopes of your dollars. These companies are Google's customers because they pay (and compete) for your attention which Google owns while you search.

iii. The Products

Viable "prediction products" forecast our thoughts, feelings, and anticipated actions based on data that are processed by machine intelligence. These products are heavily guarded from competitors and the general public. The goal is pseudo-certainty: as prediction products become more certain, more online commerce and other activity will occur.

For example, suppose a Facebook user follows several professional golfers. Suppose further that the other Facebook users this user interacts with the most (i.e., his "friends") also follow professional golfers. Facebook, using its machine intelligence, can likely predict that this user is more likely to purchase the latest golf gadget than a Facebook user who never interacts with any golf-related pages. If a company, say Gertrude's Great Golf Gadgets, wants to advertise its products on Facebook, it will purchase this prediction (i.e., the likelihood that a given number of users will click on its advertisements) from Facebook. In turn, Facebook will sell this prediction and the accompanying space on a user's newsfeed to the purchasing company.

These companies want to advertise to Facebook users with the highest likelihood of clicking on their advertisement and purchasing their products; they want the most click-through bang for their Facebook buck. Thus, it is in Facebook's best interest to know its users and predict their behavior. By refining their "prediction products" through additional surveillance and more users' data, Facebook can provide better "prediction products" to its customers.

iv. The Marketplace

Although surveillance capitalism was initially limited to advertisers, "behavioral futures markets" are now open to anyone—advertiser, businessperson, politician, etc.—keenly interested in influencing future behavior. In the same way that mass production was not confined to automobile manufacturers, sur-

veillance capitalism will not be limited to online advertising.

At its fundamental level, a marketplace connects buyers and sellers. A parent desires to purchase milk for his child without raising a dairy cow; a dairy farmer wishes to sell its milk in bulk without dealing with customers individually. Solution: the dairy farmer sells its milk to the grocery store (operating as the marketplace) and the parent purchases the milk on his way home from work.

Surveillance capitalists are both the marketplace and the seller. As discussed, when a user interacts on Facebook (post, like, share, scroll, click, etc.) he or she creates "behavioral surplus" that Facebook can capture and package into "prediction products." Facebook, operating as a seller, then sells these "prediction products" (i.e., advertisement space on a user's newsfeed) to the highest bidder. However, Facebook, operating as the marketplace, decides when, where, and how often to display this advertisement. Just like the grocery store decided to place the milk in the very back of the store,[23] so too can Facebook strategically place these advertisements on its users' newsfeeds.

In sum, surveillance capitalists capture the "behavioral surplus" created by its users, manufacture this raw material into "production products," and ultimately control the "behavioral surplus marketplace" where these "production products" are sold to the highest bidder. The wilderness of the 5:53-P.M.-grocery-store crowd seems tame compared to the frontier of surveillance capitalism.

b. A Whole New Problem: Welcome to the Frontier of Surveillance Capitalism

Congress' twentieth-century understanding of the internet is no longer applicable to today's Orwellian milieu. Children have shifted from "familiar fill-in-the-blank questionnaires" to today's trendy—and entrenched—social media sites. This shift represents much more than a "kids will be kids" market analysis; this is more than scoffing about how today's children are glued to their screens; it represents a vast, unsettled frontier. A child's every movement across the internet—from a Santa-gifted iPad to a school-issued Chromebook—is hunted, captured, prodded, and aggregated before being shipped off to the highest bidder.

Researchers have shown that members of Generation Z depend on four to five social media platforms for "psychological sustenance." Countless studies have documented the adverse effects social media has on children and teenagers (particularly on young women) including anxiety, body-image issues, and loneliness. Though today's children and teenagers are spending more time online and "connected" to their peers, this "connection" has ultimately deteriorated any sense of actual connection to themselves or the outside world; such disconnect encourages users to scroll, post, interact, and share even more, thus perpetuating the cycle. This vicious cycle is all by design.[24]

Moreover, internet users are generally unaware of how tech companies use their data. Out of blissful ignorance, users often trust that the tech companies are acting in the users' best interest. Even users that are aware of the persistent data collection are indifferent toward these companies, often claiming that such collection is necessary for our beloved phones and apps to work as well as we expect them to.

IV. Proposed Adjustments

Current and future generations deserve protection from surveillance capitalists. Reevaluating the framework by which today's social media use and online activity is understood will contribute to the burgeoning activism surrounding online privacy protection. As the previous section outlined, surveillance capitalism fundamentally alters the way we interact online and presents unprecedented problems for today's children. As COPPA enters its third decade, updating its provisions in light of surveillance capitalism becomes imperative.

The issue has been framed, the stage set, the gauntlet laid. The following three proposals address the need for more protection for children and are offered in hopes of advancing the online-privacy rights conversation. Given the gradual regulation of the internet's rapid metamorphosis, these proposals will undoubtedly contain overlooked and outdated issues in the coming years.

However, the conversation must continue—not only to educate the uninformed, but to protect the unaware.

1. Increase the Penalty

Until the monetary penalties exceed the profiteering of children's behavioral data, companies will continue to violate COPPA, and the associated penalties will remain just another cost of doing business. Discovering the monetary value of children's online behavioral data is the main barrier from determining the appropriate penalty. A framework shift from basic data collection to "behavioral surplus" is required to properly regulate these companies. In the absence of such information, Congress could adopt a two-tiered approach to fines: a set dollar amount or a percentage of the perpetrator's annual revenue, whichever is greater, with increasing percentages for repeat offenders. Without severe penalties, "surveillance capitalists are impelled to pursue lawlessness" and "vigorously lobby to kill online privacy protection . . . because such laws are existential threats to the frictionless flow of behavior surplus."[25]

2. Increase the Age

COPPA's minimum age requirement should be increased to eighteen. There is a reason that children are not allowed to vote, enlist in the military, drive, consume tobacco, or drink alcohol: a child's capacity to understand consequences develops with time. As such, companies should not exploit a child's behavioral data until he or she has turned eighteen. Adults can protect themselves from online manipulation, but society must protect children.

3. Increase the Stakes

The manufacturing of "prediction products" from children's behavioral data should be criminalized as another form of child abuse. In the seminal case, *Packingham v. North Carolina*, the U.S. Supreme Court held that a North Carolina law prohibiting registered sex offenders from accessing a "commercial social networking Web site" was too broad and therefore violated the First Amendment.[26] However, the Court noted:

> While we now may be coming to the realization that the Cyber Age is a revolution of historic proportions, we cannot appreciate yet its full dimensions and vast potential to alter how we think, express ourselves, and define who we want to be. The forces and directions of the Internet are so new, so protean, and so far reaching that courts must be conscious that what they say today might be obsolete tomorrow.[27]

The Court further observed that all new technologies, including social media, will be "exploited by the criminal mind" and "become instruments used to commit serious crimes."[28] The Court suggested that a more narrowly tailored law prohibiting registered sex offenders or other bad actors from abusing children online would not be unconstitutional.[29]

The concurring opinion takes a step further by stating that safeguarding the psychological well-being of a minor is necessary even if laws must contravene constitutional rights.[30] Moreover, States have a compelling interest to prohibit online child abuse because bad actors can—and will continue to—use the internet to exploit children.[31]

V. Current Exemplar and Concluding Thoughts

Currently, there is a bill in the United States Senate entitled "Kids Online Safety Act," which strives to provide more online protection for children.[32] The bill addresses many of the concerns discussed in this article and is a welcomed attempt to foster more conversation around this issue. Legislators cannot adequately regulate the "new logic of accumulation" without understanding how online behavioral data are manipulated into "prediction products." This bill requires online platforms to provide either minors or their parents (or both) the ability to "opt out of algorithmic recommendation systems that use a minor's personal data" and is certainly a step in the right direction.

The California Consumer Privacy Act (CCPA) is a current exemplar of how governments should respond to the ascension of surveillance capitalism.[33] The CCPA creates a statutory right for consumers to request any personal information that a business collects and requires the business to disclose that information to the consumer. Furthermore, the CCPA allows the consumer to opt-out of having such personal information sold to third parties.

Surveillance capitalists freely capture our attention, patterns, and other "behavioral surplus" as raw materials.

Surveillance capitalists freely capture our attention, patterns, and other "behavioral surplus" as raw materials. They then manufacture these raw materials in "prediction products" by using highly sophisticated algorithms. Finally, these tech companies sell their "prediction products" (digital space and click-through proclivity) to the highest bidder, leaving us with apps to update, pages to refresh, and newsfeeds to scroll. These companies will ultimately become better at capturing additional "behavioral surplus" and refining their ability to influence our emotions and actions.

Children must be protected as society begins surveying the frontier of surveillance capitalism. Leaders in every sector of society must continue discussing the issues related to internet usage and social media. Despite the constant connection to today's online world, we are discontent and disconnected. Children are no different; they will soon enter the "real world," knowing no other world aside from their screens. Understanding the "new logic of accumulation" is imperative to effectuate meaningful change for today's consumers and tomorrow's leaders.

---

* Originally published as, "*Protecting Children in the Frontier of Surveillance Capitalism,*" 27 Rich. J.L. & Tech., no. 2, 2021. This article has been substantively republished (with updates and revisions) in this Journal with permission from the Richmond Journal of Law & Technology. Many thanks are still owed to the 2020-21 Richmond JOLT Editorial Staff for their invaluable comments and edits.

** J.D., 2021, Texas A&M Univ. School of Law; B.A., 2016, Univ. of Texas at Austin. Associate Attorney at McMahon Surovik Suttle, P.C. in Abilene, Texas. Winner of the State Bar of Texas Consumer and Commercial Law Section 2020 Craig Jordan Writing Competition. This paper is dedicated to my sons: you are fiercely loved. To Wayne C. Watson: thank you for your encouragement (during all stages of life) and ongoing mentorship (through the many stages to come). All errors, omissions, and missed steaks are my own.

1 Rachael Malkin, Comment, *How the Children's Online Privacy Protection Act Affects Online Businesses and Consumers of Today and Tomorrow*, 14 Loy. Consumer L. Rev. 153, 153 (2002).

2 *See generally Rebecca Lipman, Online Privacy and the Invisible Market for Our Data, 120* Pa. State L. Rev. 777 (2016) (explaining how data brokers aggregate data about consumers to create relevant ads).

3 *See, e.g.*, Matthew Rosenberg et al., *How Trump Consultants Ex-*

ploited the Facebook Data of Millions, N.Y. Times (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [https://perma.cc/4QEH-LP59] (describing how Cambridge Analytica harvested data from the Facebook profiles of more than 50 million users to enable the Trump campaign to target key voters).

4 *Watch generally* The Social Dilemma (Exposure Labs 2020). If prone to distraction, visit https://www.thesocialdilemma.com.

5 *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 204–05 (1890).

6 *About the FTC,* Fed. Trade Comm'n, https://www.ftc.gov/about-ftc [https://perma.cc/56F6-VVV9].

7 Children's Online Privacy Protection Act, 15 U.S.C. § 6502; 16 C.F.R. § 312.1–.13; *Complying with COPPA: Frequently Asked Questions*, Fed. Trade Comm'n § A(1) (July 2020), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0 [https://perma.cc/9C9K-BN5V] [hereinafter *COPPA FAQs*].

8 *COPPA FAQs,* § A(9) (citations omitted).

9 *See* 16 C.F.R. §§ 312.2–312.3 (emphasizing that the information must come from the child in order to fall under the statutory requirements).

10 *COPPA FAQs.*

11 *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, Fed. Trade Comm'n (July 24, 2019) https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/2YTJ-G684].

12 *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law,* Fed. Trade Comm'n (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations [https://perma.cc/2LMU-ZWXN].

13 Patrick Thomas, *TikTok Settles with FTC Over Data Collection from Children*, Wall St. J. (Feb. 27, 2019, 4:36 PM), https://www.wsj.com/articles/tiktok-settles-with-ftc-over-data-collection-from-children-11551303390 [https://perma.cc/3W47-AJP8].

14 If not, it's okay to come out from under your rock now. Well, on second thought…

15 *Privacy Policy*, TikTok (June 2, 2021) https://www.tiktok.com/legal/privacy-policy?lang=en#privacy-us.

16 Kevin Poulsen & Robert McMillan, *TikTok Tracked User Data Using Tactic Banned by Google*, Wall St. J. (Aug. 11, 2020), https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738 [https://perma.cc/HU7J-SECU] ("The MAC address is useful to advertising-driven apps because it can't be reset or altered, allowing app makers and third-party analytics firms to build profiles of consumer behavior that persist through any privacy measure short of the owner getting a new phone. The [FTC] has said MAC addresses are considered personally identifiable information under the Children's Online Privacy Protection Act.").

17 Content moderation is also a huge issue for these companies. *See, e.g.,* Bobby Allen*, Former TikTok moderators sue over emotional toll of 'extremely disturbing' videos,* NPR (March 24, 2022), https://www.npr.org/2022/03/24/1088343332/tiktok-lawsuit-content-moderators

18 *See generally* George Orwell, *1984* 332 (1949) ("We know that no one ever seizes power with the intention of relinquishing it. Power is not a means; it is an end. One does not establish a dictatorship in order to safeguard a revolution; one makes the revolution in order to establish the dictatorship.").

19 Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (2019).

20 Zuboff, at 93–96.

21 Zuboff, at 94.

22 *See generally Investigation: How TikTok's Algorithm Figures Out Your Deepest Desires,* Wall Street Journal (July 21, 2021), https://www.wsj.com/video/series/inside-tiktoks-highly-secretive-algorithm/investigation-how-tiktok-algorithm-figures-out-your-deepest-desires.

23 Grumble, grumble.

24 Zuboff, at 448–450.

25 Zuboff, at 105.

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

27 *Id.* at 1736.

28 *Id.*

29 *See id.* at 1737 ("Though the issue is not before the Court, it can be assumed that the First Amendment permits a State to enact specific, narrowly tailored laws that prohibit a sex offender from engaging in conduct that often presages a sexual crime, like contacting a minor or using a website to gather information about a minor.")

30 *See id.* at 1739 (Alito, J., concurring).

31 *Id.* at 1740 (Alito, J., concurring).

32 Text - S.3663 - 117th Congress (2021-2022): Kids Online Safety Act, S.3663, 117th Cong. (2022), https://www.congress.gov/bill/117th-congress/senate-bill/3663/text.

33 *See* Cal. Civ. Code §§ 1798.100-.199. The EU General Data Protection Regulation (GDPR) is also another exemplar for regulating personal data and online privacy rights.