Richmond Journal of Law & Technology Volume XXVII, Issue 2

PROTECTING CHILDREN IN THE FRONTIER OF SURVEILLANCE CAPITALISM

Cole F. Watson*

Cite as: Cole F. Watson, *Protecting Children in the Frontier of Surveillance Capitalism*, 27 RICH. J.L. & TECH., no. 2, 2021.

* J.D. Candidate, 2021, Texas A&M Univ. School of Law; B.A., 2016, Univ. of Texas at Austin. This paper is dedicated to my soon-to-be-born son: you are fiercely loved. Many thanks to my wife and family for encouraging me through this process. To Ivan Escobar, Josh Jones, Ryan Cairns, and Christian Albuquerque: thank you for your much-needed insights and much-appreciated Bluebook knowledge. To the Richmond JOLT Editorial Staff: your comments and editing skills were invaluable. All errors, omissions, and missed steaks are my own."

"Come senators, congressmen
Please heed the call
Don't stand in the doorway
Don't block up the hall
For he that gets hurt
Will be he who has stalled
There's a battle outside and it is ragin'
It'll soon shake your windows and rattle your walls
For the times they are a-changin'"[1]
–Bob Dylan

I. INTRODUCTION

[1] This article examines the ongoing technological revolution and its impact on today's consumers. In particular, this article addresses the promulgation of the Children's Online Privacy Protection Act (COPPA) in the context of "surveillance capitalism"[2] and analyzes the harms associated with social media and data collection. Finally, this paper will argue that COPPA should be revamped to better regulate the Internet of 2020. A just society ought to protect children from the lurking perils of social media.

[2] Modernity has precipitously arrived. Gone are the days of logging into or dialing up the internet. Modernity stomped over and trampled upon the internet of yesteryear, leaving society to look around and ask "What happened?" Consider Rachael Malkin's opening paragraph regarding children's "Internet" usage in 2002:

> Everyday 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,

[1] Bob Dylan, The Times They Are A-Changin' (Warner Bros. Inc. 1963).

[2] *See* discussion *infra* Section IV.a.

> ages, genders, addresses and phone numbers. Children plug in the necessary information and continue to click away.[3]

[3] 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.[4] Though children today interact over the internet in vastly different ways than two decades ago, the privacy protections afforded to these children remain unchanged.[5]

---

[3] 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); *see also* Lindsay M. Gehman, Comment, *Deleting Online Predators Act: I Thought It Was* My-*Space — How Proposed Federal Regulation of Commercial Social Networking Sites Chills Constitutionally Protected Speech of Minors*, 27 LOY. L.A. ENT. L. REV. 155, 161 (2006) ("Commercial social websites like MySpace have become extremely popular in the past few years. Students today race home after school to their computers to chat with their friends over MySpace and customize their MySpace pages. They also have the ability to post messages directly onto their friends' MySpace pages. They can post their own daily blogs—expressing their thoughts and ideas about the trivial and the philosophical alike.") (footnotes omitted).

[4] *See* Rob Lekowski, *What Lawyers Need to Know About Data Stored on Mobile Devices*, LAW TECH. TODAY (Feb. 17, 2015), https://www.lawtechnologytoday.org/2015/02/data-stored-on-mobile-devices [https://perma.cc/7UK2-GTXJ] (providing information that modern phones store); Malkin, *supra* note 3 ("[F]amiliar fill-in-the-blank questionnaires . . . request . . . names, ages, genders, addresses and phone numbers.").

[5] Malkin, *supra* note 3 ("[Children] have no idea they have just given out personal information that will ultimately be shared with dozens of other companies. They do not comprehend that they are entitled to certain privacy rights on the Internet. In fact, they may not even understand the concept of privacy."); *see* Keith Johnson, *What Is Consumer Data Privacy, And Where Is It Headed?*, FORBES (July 9, 2018, 7:45 AM), https://www.forbes.com/sites/forbestechcouncil/2018/07/09/what-is-consumer-data-privacy-and-where-is-it-headed/#654b34ablbcl [https://perma.cc/76R6-3HRT] (discussing how personal data protection is often obfuscated in a convoluted privacy policy).

[4] Society sits at an unprecedented juncture of data collection and privacy rights.[6] Millennials will be the last generation to recall a time before the internet's proliferation.[7] A wider audience is beginning to understand that personal data is constantly collected, "anonymized,"[8] and controlled by companies. Although collected data can benefit the user,[9] companies can also use this data to shape buying habits[10] and manipulate political philosophies.[11] Criminals have begrimed the internet, targeting susceptible

[6] *Cf.* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. R. 805, 810, 879–80 (2016) ("The Internet of Things has just begun to shape our lives . . . . If billions of sensors filled with personal data fall outside of Fourth Amendment protections, a large-scale surveillance network will exist without constitutional limits.").

[7] Edie Meade, *The Last Analogue Generation*, MEDIUM (Feb. 14, 2020), https://medium.com/age-of-awareness/the-last-analogue-generation-f899cf40975d [https://perma.cc/7JCJ-8HRE].

[8] Nick Wells & Leslie Picker, *'Anonymous' Data Might Not Be So Anonymous, Study Shows*, CNBC (July 23, 2019 2:21 PM), https://www.cnbc.com/2019/07/23/anonymous-data-might-not-be-so-anonymous-study-shows.html [https://perma.cc/L5SH-UP4M]; Luk Arbukle, *Aggregated Data Provides a False Sense of Security*, IAPP (Apr. 27, 2020), https://iapp.org/news/a/aggregated-data-provides-a-false-sense-of-security/ [https://perma.cc/5U79-9JG7].

[9] *See generally* YAN LAU, FED. TRADE COMM'N, A BRIEF PRIMER ON THE ECONOMICS OF TARGETED ADVERTISING (2020) (describing how advertising can benefit consumers by presenting products that match their interests).

[10] *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); Avi Goldfarb & Catherine E. Tucker, *Online Display Advertising: Targeting and Obtrusiveness*, 30 MKTG. SCI. 389 (2011) (explicating how highly visible and contextually targeted ads increase interaction between consumers and products).

[11] *See, e.g.*, Matthew Rosenberg et al., *How Trump Consultants Exploited 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).

populations online[12] and spreading false information about the Covid-19 pandemic.[13]

[5] The lives of today's children are often 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 experiment until it is too late. As the most vulnerable and impressionable population in our society, children deserve the highest levels of legal protection.[14]

[12] *E.g.*, Lisa Weintraub Schifferle, *Grandparent Scams in the Age of Coronavirus*, FED. TRADE COMM'N: CONSUMER INFO. (Apr. 3, 2020), https://www.consumer.ftc.gov/blog/2020/04/grandparent-scams-age-coronavirus [https://perma.cc/2ACW-5BQX] (describing common coronavirus-related scams used on elderly populations); Cristina Miranda, *Scammers Are Using COVID-19 Messages to Scam People*, FED. TRADE COMM'N: CONSUMER INFO. (Apr. 10, 2020), https://www.consumer.ftc.gov/blog/2020/04/scammers-are-using-covid-19-messages-scam-people [https://perma.cc/8PXK-76ZL] (explicating different COVID-19 scams).

[13] *Cf.* U.N. Dep't of Glob. Commc'ns, *U.N. Tackles 'Infodemic' of Misinformation and Cybercrime in COVID-19 Crisis* (Mar. 31, 2020), https://www.un.org/en/un-coronavirus-communications-team/un-tackling-'infodemic'-misinformation-and-cybercrime-covid-19 [https://perma.cc/8F5Q-36LC] ("[I]nfodemics . . . can spread misinformation, disinformation and rumours during a health emergency . . . [and] can hamper an effective public health response and create confusion and distrust among people."); Jason Murdock, *Most COVID-19 Misinformation Originates on Facebook, Research Suggests*, NEWSWEEK (July 6, 2020, 9:31 AM), https://www.newsweek.com/facebook-covid19-coronavirus-misinformation-twitter-youtube-whatsapp-1515642 [https://perma.cc/2ZTV-P2FN].

[14] *See infra* Section IV.

II. RECLAIMING PRIVACY

[6] Privacy is a long-established right.[15] However, in comparison, consumer protection rights are relatively new.[16] President Woodrow Wilson created the Federal Trade Commission (FTC) in 1914 to prevent unfair competition.[17] Operating within this framework, additional legislation broadened the FTC's regulatory power to protect the privacy rights of consumers by prohibiting deceptive practices involving consumers' personal information.[18]

A. History of COPPA

[7] Toward the end of the twentieth century, as more children began accessing the internet, Congress enacted the Children's Online Privacy Protection Act (COPPA).[19] COPPA requires the FTC to issue and enforce

[15] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 204–05 (1890) ("If the fiction of property in a narrow sense must be preserved, it is still true that the end accomplished by the gossip-monger is attained by the use of that which is another's, the facts relating to his private life, which he has seen fit to keep private.").

[16] *See* Mark E. Budnitz, *The Development of Consumer Protection Law, the Institutionalization of Consumerism, and Future Prospects and Perils*, 26 GA. ST. UNIV. L. REV. 1147, 1149 (2012) (discussing the lack and inadequacy of consumer protection laws); Comment, *Translating Sympathy for Deceived Consumers into Effective Programs for Protection*, 114 UNIV. PA. L. REV. 395, 395–96 (1966) ("With the tremendous expansion of consumer credit since World War II and the accompanying 'nefarious, unscrupulous and improper practices [that] exist in certain areas of consumer credit,' an acute necessity for protecting consumers has arisen.") (footnote omitted).

[17] *Our History*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/our-history [https://perma.cc/K6AW-X2SB].

[18] *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc [https://perma.cc/56F6-VVV9].

[19] Children's Online Privacy Protection Act, 15 U.S.C. § 6502; *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*].

regulations concerning online privacy for children under the age of thirteen.[20] COPPA's strives to provide parental control over information collected from their children online.[21] COPPA applies to operators of commercial websites for kids and websites that act with an "actual knowledge" that they are collecting, using, or disclosing "personal information"[22] from children under the age of thirteen.[23] Operators must post a clear privacy policy, obtain verifiable parental consent, provide parents access to delete their child's information, and maintain the confidentiality of collected information.[24] After the retained personal information has fulfilled its intended purpose, operators must destroy the information to prevent unauthorized access.[25]

[8] COPPA does not apply to information collected *about* children, only *from* children.[26] However, the FTC fully expects operators to confidentially secure any information obtained from parents in the course of obtaining parental consent.[27] Regarding teenage users, the FTC further explains:

> In enacting [COPPA], Congress determined to apply the statute's protections only to children under 13, recognizing

[20] *Id.*

[21] *COPPA FAQs*, *supra* note 19, § 11; *see* 16 C.F.R. § 312.5(a) (2020).

[22] *Id.* § 312.2 (2020) (including identifiable information such as an individual's name and address as well as "persistent identifiers" such as cookies, Internet Protocol (IP) addresses, or a device's serial number).

[23] *COPPA FAQs*, *supra* note 19, § A(1); 16 C.F.R. § 312.3.

[24] *COPPA FAQs*, *supra* note 19, § A(1).

[25] *Id.*

[26] *Id.* § A(8); *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).

[27] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,902 (Nov. 3, 1999) (to be codified at 16 C.F.R. pt. 312) (emphasis added).

> 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.[28]

[9] COPPA does not inhibit a child's access to certain websites thereby leaving a child's parent or school responsible for filtering internet access.[29] 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."[30] Foreign-based websites must also comply with COPPA as do U.S.-based websites that collect information from foreign children.[31]

B. Ongoing Privacy Violations

[10] Online privacy violations continue to occur as companies disregard consumer protection laws.[32] Although tech companies pay tremendous amounts of money to settle allegations with the FTC, the quasi-punishment

[28] *COPPA FAQs*, *supra* note 19, § A(9) (citations omitted).

[29] *Id.* § A(11).

[30] *Id.* § B(2).

[31] *Id.* § B(7).

[32] *See* Ryan Tracy, *Big Tech's Power Comes Under Fire at Congressional Antitrust Hearing*, WALL ST. J. (July 29, 2020, 7:29 PM), https://www.wsj.com/articles/tech-ceos-defend-operations-ahead-of-congressional-hearing-11596027626 [https://perma.cc/WB48-4GB3] ("Lawmakers whipsawed between topics, from how the companies moderate social media posts to the tactics they used to gain sizable positions in markets from digital advertising to e-commerce.").

these companies may not fit the alleged violation.[33] Furthermore, unknown and upcoming companies are just as likely to violate privacy protection laws as the "Tech Titans."[34]

1. Facebook's FTC Settlement

[11] Facebook's recent settlement with the FTC illuminates the degradation of consumers' online privacy. Based on allegations that Facebook violated its 2012 FTC privacy order, Facebook assented to an unprecedented $5 billion settlement with the FTC.[35] Referring to the settlement, FTC Chairman, Joe Simons, stated that "[t]he relief is designed not only to punish future violations but, more importantly, to change Facebook's entire privacy culture to decrease the likelihood of continued violations."[36] The Assistant Attorney General for the Department of Justice Civil Division reiterated that "[t]he Department of Justice is committed to protecting consumer data privacy and ensuring that social media companies like Facebook do not mislead individuals about the use of their personal information."[37] The FTC determined that "Facebook repeatedly used deceptive disclosures and settings to undermine users' privacy preferences" in violation of a previous FTC order.[38] Facebook failed to inform its users that third-party apps collected data from Facebook users' "friends" without

[33] *See infra* Section IV.c.i.

[34] *See* Tracy, *supra* note 32 (referring to Amazon, Facebook, Apple, and Google); *see infra* Section II.b.ii.

[35] *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].

[36] *Id.*

[37] *Id.*

[38] *Id.*

receiving proper consent.[39] To ensure future compliance, the FTC order established an independent privacy committee of Facebook's board of directors thereby curtailing CEO Mark Zuckerberg's adamantine control.[40] These amendments are now included in the 2012 FTC privacy order.[41]

2. YouTube and Other Violators

[12] In 2019, YouTube paid $170 million to settle allegations by the FTC that the company illegally collected personal information from children without their parents' consent.[42] Persistent identifiers—or "cookies"—were used to track children who viewed child-directed channels across the internet without first notifying parents and receiving meaningful consent.[43] Even though several channel owners directed their content to children—and despite YouTube marketing its popularity with children to prospective corporate clients—YouTube refused to acknowledge that it violated COPPA.[44]

[13] Channel owners can monetize their channel by allowing YouTube to disseminate "behaviorally targeted advertisements" to their viewers.[45]

---

[39] *See id.*

[40] *Id.*

[41] *See FTC Gives Final Approval to Modify FTC's 2012 Privacy Order with Facebook with Provisions from 2019 Settlement*, FED. TRADE COMM'N (Apr. 28, 2020), https://www.ftc.gov/news-events/press-releases/2020/04/ftc-gives-final-approval-modify-ftcs-2012-privacy-order-facebook [https://perma.cc/BR9J-HZHT].

[42] *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].

[43] *See id.*

[44] *See id.*

[45] *Id.* (emphasis added); *see infra* Section III.a (discussing Professor Shoshana Zuboff's "surveillance capitalism," considering Google, YouTube's parent company, as the

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.[46] Despite the ubiquity of its underage viewers, YouTube denied its need to comply with COPPA.[47] 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.[48] Though Facebook[49] and Google[50] are the most notorious violators of privacy laws, the FTC has also settled other allegations of privacy and data violations with Cambridge

"pioneer" of the concept, and concluding with an optimistic view regarding the increasing accessibility of exploiting "behavioral future markets").

[46] *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, *supra* note 42.

[47] *Id.*

[48] *Id.*

[49] *See supra* Section II.b; *see also* Brent Kendall & Emily Glazer, *FTC Considering Deposing Top Facebook Executives in Antitrust Probe*, WALL ST. J., (July 17, 2020, 5:57 PM), https://www.wsj.com/articles/ftc-considering-deposing-top-facebook-of [https://perma.cc/5MA2-VKTL] ("Facebook is one of a handful of tech giants in the government's crosshairs amid concerns they are too powerful and stifle competition.").

[50] *See generally* J.H. Jennifer Lee et. al., *Consumer Protection in the New Economy: Privacy Cases in E-Commerce Transactions or Social Media Activities*, 73 CONSUMER FIN. L. Q. REP. 6 (2019) (stating that Google repeatedly violates privacy laws); Raizel Liebler & Keidra Chaney, *Google Analytics: Analyzing the Latest Wave of Legal Concerns for Google in the U.S. and the E.U.*, 7 BUFF. INTELL. PROP. L.J. 135 (2010) (stating that Google repeatedly violates privacy laws).

Analytica,[51]Twitter,[52] Snapchat,[53] HyperBeard,[54] Unixiz, Inc.,[55] and Retina-X Studios.[56]

3. TikTok

[14] TikTok captures the majority of today's privacy-concerned headlines.[57] TikTok is a social media application that allows users to create

[51] *See FTC Grants Final Approval to Settlement with Formal Cambridge Analytica CEO, App Developer over Allegations they Deceived Consumers over Collection of Facebook Data*, FED. TRADE COMM'N (Dec. 18, 2019), https://www.ftc.gov/news-events/press-releases/2019/12/ftc-grants-final-approval-settlement-former-cambridge-analytica [https://perma.cc/DA97-3MW4] (settling with Cambridge Analytica's CEO).

[52] *Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program*, FED. TRADE COMM'N (June 24, 2010), https://www.ftc.gov/news-events/press-releases/2010/06/twitter-settles-charges-it-failed-protect-consumers-personal [https://perma.cc/AT8H-5F4H].

[53] *Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False*, FED. TRADE COMM'N (May 8, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were [https://perma.cc/RZ7B-T6WL].

[54] *Developer of Apps Popular with Children Agrees to Settle FTC Allegations It Illegally Collected Kids' Data Without Parental Consent*, FED. TRADE COMM'N (June 4, 2020), https://www.ftc.gov/news-events/press-releases/2020/06/developer-apps-popular-children-agrees-settle-ftc-allegations-it [https://perma.cc/DE5N-JP3T].

[55] *FTC Alleges Operators of Two Commercial Websites Failed to Protect Consumers' Data*, FED. TRADE COMM'N (Apr. 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/04/ftc-alleges-operators-two-commercial-websites-failed-protect [https://perma.cc/EUN6-LX4Q].

[56] *FTC Gives Final Approval to Settlement with Stalking Apps Developer*, FED. TRADE COMM'N (Mar. 27, 2020), https://www.ftc.gov/news-events/press-releases/2020/03/ftc-gives-final-approval-settlement-stalking-apps-developer [https://perma.cc/B3NF-ZYDQ] (noting that the developer of "'stalking' apps . . . allowed purchasers to monitor the mobile devices on which they were installed, without the knowledge or permission of the device's user.").

[57] *See* Josh Lake, *TikTok, Privacy & Security – Should it Be Banned or Sold?*,

and share short videos, often with whimsical dance moves choreographed to popular songs.[58] After launching in 2016, TikTok has accumulated more than 2.2 billion users worldwide and is valued at over $100 billion.[59] TikTok's predecessor, Musical.ly, already settled with the FTC regarding previous COPPA violations.[60] ByteDance, Ltd., TikTok's parent company, paid $5.7 million to settle the allegations with the FTC.[61] In recent months, U.S. officials have been concerned that TikTok will be obligated to relinquish user data to the Chinese government.[62] TikTok collects a plethora

COMPARITECH (Aug. 10, 2020), https://www.comparitech.com/blog/vpn-privacy/tiktok-privacy-security/ [https://perma.cc/Q8WG-CJRW].

[58] *See* Deborah Dsouza, *What is TikTok?*, INVESTOPEDIA (Feb. 10, 2020), https://www.investopedia.com/what-is-tiktok-4588933 [https://perma.cc/985U-EJBU].

[59] Liza Lin & Shan Li, *TikTok Weighs Pullback from China - WSJ*, MARKETSCREENER (July 10, 2020, 3:48 AM), https://www.marketscreener.com/quote/stock/TWITTER-38965267/news/TikTok-Weighs-Pullback-From-China-WSJ-30904810/ [https://perma.cc/BZ9G-GUCB].

[60] *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law*, FED. TRADE COMM'N (Feb. 27, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc [https://perma.cc/V32X-39KC].

[61] 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].

[62] John D. McKinnon & Shan Li, *TikTok Could Be Tougher Target for Trump Administration*, WALL ST. J. (July 26, 2020), https://www.wsj.com/articles/tiktok-could-be-tougher-target-for-trump-administration-11595755800 [https://perma.cc/52LB-7Y58] ("U.S. officials say they are concerned that TikTok, owned by Beijing-based ByteDance Ltd., could pass on the data it collects from Americans streaming videos to China's authoritarian government. TikTok has said it would never do so. U.S. officials also are increasingly concerned about the risk of misinformation and Chinese propaganda being spread on the app."); *See* Liza Lin & Eva Xiao, *TikTok Maker Seeks to Strike Balance as China, U.S. Step Up Geopolitical Pressure*, WALL ST. J. (July 7, 2020), https://www.wsj.com/articles/tiktok-to-pull-out-of-hong-kong-after-china-imposed-national-security-law-11594096439 [https://perma.cc/L2ZU-8LS7] ("The pressures TikTok faces reflect the continued fracturing of the internet along geopolitical lines amid rising tensions between the U.S. and China."); Robert McMillan & Liza Lin, *TikTok User*

of user information including; a user's location, internet address, copied clipboard text,[63] browsing history, messages, and contacts.[64] Most recently, a *Wall Street Journal* analysis found that TikTok collected unique identifiers—"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.[65] As a result of this additional scrutiny, ByteDance, Ltd., is considering changing its corporate structure or establishing a headquarters outside of China.[66]

Data: What Does the App Collect and Why Are U.S. Authorities Concerned?, WALL ST. J. (July 7, 2020), https://www.wsj.com/articles/tiktok-user-data-what-does-the-app-collect-and-why-are-u-s-authorities-concerned-11594157084 [https://perma.cc/RB6J-4K3E] ("U.S. officials are concerned that the Chinese government is potentially building a vast database of information that could be used for espionage—identifying U.S. government employees who might be susceptible to blackmail, for example . . . .").

[63] *But cf.* Sean Kim, *Protecting privacy on TikTok*, TIKTOK NEWSROOM (July 22, 2020), https://newsroom.tiktok.com/en-us/protecting-privacy-on-tiktok [https://perma.cc/S3HH-G46H] ("Starting with the new update, TikTok will only allow a third-party app to access a users [sic] clipboard when an action is expressly initiated by a user, such as sharing to Snapchat or Instagram Stories.").

[64] *Privacy Policy*, TIKTOK (Jan. 1, 2020) https://www.tiktok.com/legal/privacy-policy?lang=en#privacy-us [https://perma.cc/5F5R-286P] ; *see* Yang Liu et al., *Case Study: A Chinese Social Video App TikTok Violates Children's Privacy Laws in the United States*, 23 No. 9 J. INTERNET L. 1, 16 (2020).

[65] 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.").

[66] Lin & Li, *supra* note 59 ("Officials in several countries have expressed concerns with the large volumes of user data TikTok collects . . . Any change to the corporate structure has to be significant enough to separate TikTok from any entanglements with mainland China, and has to cut off mainland Chinese staff from accessing user data . . . .").

[15] Children, tweens, and teenagers commonly use TikTok.[67] Unfortunately, this has made children increasingly vulnerable to sexual predators.[68] U.S. Senators have urged the FTC to further investigate TikTok for violating its 2019 settlement by retaining children's data.[69] Parental complaints have also prompted the FTC to reopen its investigation, alleging that TikTok was aware that children under the age of 13 were signing up for, and using, the application without parental approval and oversight[70]

[67] *See generally House Republicans press TikTok on use of kids' data, ties to Beijing*, REUTERS (May 21, 2020), https://www.reuters.com/article/us-tiktok-privacy-children-republicans-idUSKBN22X26P [https://perma.cc/N897-K35K] (noting that two U.S. House of Representative Republicans, "wrote a letter to the founder of the popular video sharing app TikTok on Thursday, asking about potentially illegal use of data about children . . . ."); Stephanie Thurrott, *What is TikTok? And is it safe? A guide for clueless parents*, NBC NEWS (Oct. 21, 2019), https://www.nbcnews.com/better/lifestyle/what-tiktok-guide-clueless-parents-ncna1066466 [https://perma.cc/3UFQ-FBTX] (describing the interest that children have in TikTok); *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law, supra* note 60 ("The operators of the Musical.ly app were aware that a significant percentage of users were younger than 13 and received thousands of complaints from parents that their children under 13 had created Musical.ly accounts, according to the FTC's complaint."); Yang Liu et al., *Case Study: A Chinese Social Video App TikTok Violates Children's Privacy Laws in the United States*, 23 No. 9 J. INTERNET L. 1, 16 (2020) (acknowledging that younger individuals, especially in America, use TikTok).

[68] *See, e.g.*, *Fresno Man Admits Sexual Exploitation of at Least 50 Children Through Multiple Social Media Apps*, DEPT. OF JUSTICE (May 15, 2020), https://www.justice.gov/usao-edca/pr/fresno-man-admits-sexual-exploitation-least-50-children-through-multiple-social-media [https://perma.cc/YE3Z-AMX9] ("Blanco used Snapchat, Kik, Musical.ly (Tik Tok), and other applications to communicate with minor females for the purpose of having those minors create and transmit to him image of themselves engaged in sexually explicit conduct.").

[69] *See* Henry Kenyon, *Senators urge FTC to investigate reports of privacy violations by TikTok*, CQ ROLL CALL, June 1, 2020, at 1, 2020 WL 2832616 ("A bipartisan group of senators urged the Federal Trade Commission to investigate Tik Tok on grounds the video sharing social media platform violated young users' privacy and failed to abide by a 2019 settlement with the Commission.").

[70] *See* Kim Lyons, *TikTok hit with complaint from child privacy advocates who say it's still flouting the law*, THE VERGE, (May 14, 2020), https://www.theverge.com/2020/5/14/21258502/tiktok-complaint-child-privacy-ftc [https://perma.cc/57XS-H3FZ] ("TikTok

(despite TikTok limiting its platform to people 13 years of age or older).[71] As data collection escalates, privacy rights should not become the norm. Now is the time to reclaim the right to privacy by preventing companies from monetizing children's online data.

III. CONTEXTUALIZING THE PROBLEM OF PRIVACY

[16] The right to privacy transforms with each generation. George Orwell's 1984 is often cited when discussing the intersection of technology and privacy rights.[72] The error is thinking that Orwell's imagination is still a way's away— in the future, close but not quite here, or otherwise confined to its pages written decades ago. Of course, the reality is that "Big Brother" is actually Big Tech and *1984*'s plot is yesterday's news. While older generations gradually discover their online activity is under constant surveillance, younger generation's right to online protection is vaporizing.

paid a $5.7 million fine to the FTC in February 2019 over allegations that an earlier version of its app, . . . allow[ed] users younger than 13 to sign up without parental consent."); *Compare Privacy Policy for Younger Users*, TIKTOK (Jan. 2020), https://www.tiktok.com/legal/privacy-policy-for-younger-users?lang=en [https://perma.cc/T2EZ-LS45] (making no reference to parental consent), *with Terms of Service*, TIKTOK (Feb. 2019), https://www.tiktok.com/legal/terms-of-use?lang=en [https://perma.cc/UVS7-RH2Q] ("If you are under age 18, you may only use the Services with the consent of your parent or legal guardian.").

[71] *Terms of Service*, TIKTOK (Feb.2019), https://www.tiktok.com/legal/terms-of-use?lang=en, [https://perma.cc/9JTD-VA72] (showing that the terms of service state that users must be 13 years of age or older).

[72] *See generally* GEORGE ORWELL, 1984 (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.").

A. Surveillance Capitalism Defined

[17] In her seminal work, *The Age of Surveillance Capitalism*, Professor Shoshana Zuboff defines "surveillance capitalism" as "the new logic of accumulation."[73] 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 improvement, 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.[74]

[18] Professor Zuboff provides a framework for understanding the novelty of surveillance capitalism: (1) the logic, (2) the means of production, (3) the products, and (4) the marketplace.[75] Google is considered the "pioneer" of surveillance capitalism and their business practice can be traced through the proliferation of its online advertising business model.[76]

---

[73] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 8 (2019).

[74] *Id.*

[75] *Id.* at 93–96.

[76] *Id.* at 63–67; *See generally* Kayla McKinnon, Comment, *Nothing Personal, It's Just Business: How Google's Course of Business Operates at the Expense of Consumer Privacy*, 33 J. MARSHALL J. INFO. TECH. & PRIVACY L. 187, 187–88 (2018).

1. The Logic

[19] Google's discovery of "behavioral surplus" allowed the company to "translate its nonmarket interactions" into "prediction products" readily available for advertisers.[77] Prediction products are "surveillance assets" which ultimately produce "surveillance revenues" and "surveillance capital."[78] The adage "[i]f a service is free, you're the product,"[79] is no longer true. "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*."[80] 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."[81]

[77] Zuboff, *supra* note 73, at 93–94; *See* Amy Tracy, *Technology Law-Great Google-Y Moogley: The Effect and Enforcement of Click Fraud and Online Advertising*, 32 UNIV. ARK. L. REV. 347, 349–53 (2010).

[78] ZUBOFF, *supra* note 73, at 94.

[79] *See* Scott Goodson, *If You're not Paying for it, you become the Product*, FORBES (Mar. 5, 2012), https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/#317c03c45d6e [https://perma.cc/7QVB-7BP9] ("But the next time you're browsing the web or enjoying a video on YouTube, remember that Google is watching your every move; because that's the price you pay.").

[80] ZUBOFF, *supra* note 73, at 94.

[81] *See id.*

2. The Means of Production

[20] Machine learning and artificial intelligence are the new means of production.[82] As Google (and other surveillance capitalists) accumulate more data, their "machine intelligence" evolves and their prediction products become more accurate.[83] Indeed, Google researchers have already introduced a new "deep-neural network model" to significantly improve "clickthrough rate"[84] predictions.[85]

3. The Products

[21] Viable "prediction products" forecast our thoughts, feelings, and likely actions based on data that are processed by machine intelligence.[86] These products are heavily guarded from competitors and the general

[82] *See id.* at 95; *cf.* Bob Lambrechts, *May It Please the Algorithm*, 89 J. KAN. B. ASS'N. 36, 37 (2020) (discussing how artificial intelligence will change the legal profession); *see also* Darrell M. West & John R. Allen, *How Artificial Intelligence is Transforming the World*, BROOKINGS (Apr. 24, 2018), https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/ [https://perma.cc/LX6A-DEPJ] (discussing how artificial intelligence is shaping finance, national security, health care, and infrastructure among other industries).

[83] *See* ZUBOFF, *supra* note 73, at 95.

[84] *See generally Clickthrough Rate (CTR): Definition*, GOOGLE ADS HELP, https://support.google.com/google-ads/answer/2615875?hl=en [https://perma.cc/MKX5-DBCE] (explaining that CTR is the ratio between how many people click on a given advertisement ("clicks") and how many people saw the ad ("impressions"), and that a higher CTR means that the ad is more helpful and relevant for the particular search terms used).

[85] *See* ZUBOFF, *supra* note 73, at 95–96.

[86] *Id.* at 96.

public.[87] The goal is pseudo-certainty: as prediction products become more certain, the more online commerce will commence.[88]

4. The Marketplace

[22] Though the market was initially limited to advertisers, "behavioral futures markets" are now open to any entity—advertiser, businessperson, politician, or otherwise[89]—keenly interested in influencing future behavior.[90] In the same way that mass production was not confined to automobile manufacturers, surveillance capitalism with its new logic, means, and products will not be bridled to online advertising.[91]

B. A Whole New Problem

[23] Congress' twentieth-century understanding of the internet is no longer applicable to today's digital milieu.[92] Children have shifted from "familiar fill-in-the-blank questionnaires"[93] and "customize[d] . . .

[87] *See id.*

[88] *See id.*

[89] *Id*. *See, e.g.*, Bruno Zeller et al., *The Internet of Things–the Internet of Things or of Human Objects? Mechanizing the New Social Order*, 47 RUTGERS L. REC. 15, 19 (2020) ("[Personal data] manipulation is most evident by mega-data corporations, such as Facebook, providing the data of millions of users to Cambridge Analytica . . . to influence voters in the 2016 US Presidential Elections and the UK referendum on Brexit.").

[90] *See* ZUBOFF, *supra* note 73, at 96.

[91] *See id.*

[92] *See generally* Ariel Fox Johnson, *13 Going on 30: An Exploration of Expanding COPPA's Privacy Protections to Everyone,* 44 SETON HALL LEGIS. J. 419, 431–443 (2020) (discussing how children's use of technology has dramatically changed since COPPA's inception and the subsequent effects on children as a result).

[93] Malkin, supra note 3.

MySpace pages"[94] to today's trendy and entrenched social media sites. This transition represents much more than "stranger danger";[95] 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 often hunted, captured, prodded, and aggregated before being shipped off to the highest bidder. Welcome to the frontier of surveillance capitalism.

1. Mental and Social Development

[24] Teens are sharing more information on social media sites than they ever have before.[96] In turn, their mental health severely suffers.[97] Researchers have shown that Generation Z—"the first group of digital natives, with no memory of life before the rise of surveillance capitalism"—relies on four to five social media platforms for "psychological sustenance."[98] Researchers reported findings of "loneliness and acute disorientation that overwhelm young people when faced with disconnection from social media."[99] Given the fact that 95% of Generation Z uses smartphones and 45% are online "on a near-constant basis," it makes sense that teenagers today increasingly see themselves through their social media

[94] Gehman, supra note 3.

[95] *E.g.*, Martine Oglethorpe, *Teaching Stranger Danger in a digital world*, THE MODERN PARENT (Jan. 14, 2020, 11:35 AM), https://themodernparent.net/teaching-stranger-danger-in-a-digital-world/ [https://perma.cc/6UFR-8AKY]; *see generally* Anita L. Allen, *Minor Distractions: Children, Privacy, and E-Commerce*, 38 U. Pa. L. Rev. 751, 754-58 (2001) (discussing how the internet threatened young families almost two decades ago).

[96] Mary Madden et al., *Teens, Social Media, and Privacy*, PEW RES. CTR. (May 21, 2013), http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/ [https://perma.cc/4569-9RAK].

[97] *See* ZUBOFF, supra note 73, at 445.

[98] *Id.* at 447.

[99] *Id.*

accounts, or what researchers call an "outside-looking-in approach."[100] This phenomenon further entrenches the feelings of "disorientation and isolation" and "suggests a psychological dependency on the 'others.'"[101]

[25] Today's children are different from children two to three generations ago.[102] Psychologists denote "emerging adulthood" as the years between eighteen and the late twenties, and the essential challenge for this new "life stage" is differentiating self from others.[103] The separation between childhood and adulthood is growing in today's time: "emerging adulthood is to the twenty-first century what adolescence was to the twentieth."[104]

[26] Psychologists have said that the essential challenge of "emerging adulthood" is delineating between one's self and social peers.[105] The proliferation of social media muddles this delineation.[106] Professor Zuboff expatiates three ways the "enduring existential task of self-making"[107] is

[100] *Id.*

[101] *Id.*

[102] *Id.* at 462 (explaining that "[s]ocial media marks a new era in the intensity, density, and pervasiveness of social comparison processes, especially for the youngest among us, who are 'almost constantly online' at a time of life when one's own identity, voice, and moral agency are a work in progress. In fact, the psychological tsunami of social comparison triggered by the social media experience is considered unprecedented. If television created more life dissatisfaction, what happens in the infinite spaces of social media?").

[103] ZUBOFF, *supra* note 73, at 452; *accord* JEFFREY JENSEN ARNETT, EMERGING ADULTHOOD: THE WINDING ROAD FROM THE LATE TEENS THROUGH THE TWENTIES (2006).

[104] ZUBOFF, *supra* note 73, at 452.

[105] *Id.* at 453.

[106] *See id.* at 453–54.

[107] *Id.* at 455.

morphed by the internet's prevalence: (1) accelerated individualization, (2) online socialization, and (3) the domination of "network publics."[108] Professor Zuboff expounds further:

> Young life now unfolds in the spaces of private capital, owned and operated by surveillance capitalists, mediated by their 'economic orientation,' and operationalized in practices designed to maximize surveillance revenues. These private spaces are the media through which every form of social influence—social pressure, social comparison,[109] modeling, subliminal priming—is summoned to tune, herd, and manipulate behavior in the name of surveillance revenues. This is where adulthood is now expected to emerge.[110]

[27] Facebook has openly acknowledged that their platform is a "sensory experience of communication that helps us connect to others, without having to look away."[111] Their platform is based on the addictive nature of casino games with the intention that users enter a mental state called the "machine zone": a connection between user and device that invokes a "loss of self-awareness, automatic behavior, and a total rhythmic absorption carried along on a wave of compulsion."[112] Anyone who has scrolled their Facebook feed for an extended period of time and suddenly "snaps out of it" knows the feeling.[113]

---

[108] *See* DANAH BOYD, IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS (2014).

[109] ZUBOFF, *supra* note 73, at 455–56.

[110] *Id.* at 456.

[111] *Id.* at 448.

[112] *Id.* at 449–50; *accord* NATASHA DOW SCHÜLL, ADDICTION BY DESIGN: MACHINE GAMBLING IN LAS VEGAS 166–67 (2014).

[113] *See, e.g.*, Brian X. Chen, *You're Doomscrolling Again. Here's How to Snap Out of It*, N.Y. TIMES (July 15, 2020),

2. Data Collection

[28] Internet users are generally unaware of how tech companies use aggregated data collection. For instance, the *Journal of Social Studies Research* published a study that examined high school students' responses to the discussion of internet privacy.[114] Three startling themes emerged from the researchers' analysis of the students' responses:

> (1) students displayed a surprising trust in Facebook and Google;
> (2) students framed the issue of Internet Privacy as a conflict in values and a set of trade-offs; and
> (3) students tended to put more weight on personal consequences and responsibility than on implications for democracy in their assessment of the (acknowledged) erosion of privacy as a result of social media and Internet search engines.[115]

[29] Teenagers implicitly trust tech companies and presume that the companies are acting in the user's best interest.[116] Researchers speculated that such lackadaisical responses could stem from broader themes of tradeoffs around privacy in the post-9/11 world.[117] Americans generally accepted the increase in state surveillance as a tradeoff for increased

https://www.nytimes.com/2020/07/15/technology/personaltech/youre-doomscrolling-again-heres-how-to-snap-out-of-it.html. [https://perma.cc/HYD2-JCUY].

[114] Margaret S. Crocco et al., *"It's not like they're selling your data to dangerous people": Internet privacy, teens, and (non-)controversial public issues*, 44 J. SOC. STUD. RES. 21, 25 (2019).

[115] *Id.* at 21–33.

[116] *See id.*

[117] *See* Crocco et al., *supra* note 114 at 26–28.

protection.[118] Thus, the "cultural zeitgeist" in which these students grew up fundamentally shaped their conceptions of online privacy: "[p]erhaps the traditional valuation of privacy by adolescents needs redefinition in a media-saturated society in which young people live their lives on [social media], without much thought about the potential long-term consequences for their adulthood."[119]As another study explains:

> When asked whether [students] thought Facebook gives anyone else access to the information they share, one middle schooler wrote: 'Anyone who isn't friends with me cannot see anything about my profile except my name and gender. I don't believe that [Facebook] would do anything with my info.' Other high schoolers shared similar sentiments, believing that Facebook would not or should not share their information.[120]

[30] When similarly question, however, parents expressed deep concern over how much information companies could learn about their children simply by tracking their children's online behavior.[121]

[118] John Cohen, *Most Americans Back NSA Tracking Phone Records, Prioritize Probes over Privacy*, WASH. POST (June 10, 2013), https://www.washingtonpost.com/politics/most-americans-support-nsa-tracking-phone-records-prioritize-investigations-over-privacy/2013/06/10/51e721d6-d204-11e2-9f1a-1a7cdee20287_story.html. [https://perma.cc/5G5Q-H2F9].

[119] Crocco et al., *supra* note 114 at 28.

[120] Madden et al., *supra* note 96.

[121] *See* Madden et al., *supra* note 96; *but cf.* Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 EMORY L.J. 839, 842–44 (2017) (arguing that "sharenting," the parental act of sharing details about their child online (text, pictures, etc.), should be at the forefront of legal analysis when a parent's right to share conflicts with a child's right to privacy).

3. Sexual exploitation

[31] As an empirical matter, children's online presence increases their exposure to sexual content and solicitation.[122] Even before the rise of social media, experts warned of the proliferation of child exploitation and pornography as the internet pullulated from its nascency.[123] Sexual predators frequently use social media sites as a way to lure children into sexual conversations.[124] Despite this knowledge, internet service providers and social networking sites are likely legally inculpable.[125] Predators may

[122] *See* Adina Farrukh et al., CTR. FOR TECH. INNOVATION AT BROOKINGS, YOUTH INTERNET SAFETY: RISKS, RESPONSES, AND RESEARCH RECOMMENDATIONS, 5–6 (2014), https://www.brookings.edu/wp-content/uploads/2016/06/Youth-Internet-Safety_v07.pdf [https://perma.cc/RLM6-TVLR]; *see also* Nellie Bowls & Michael H. Keller, *Video Games and Online Chats are 'Hunting Grounds' for Sexual Predators*, N.Y. TIMES (Dec. 7, 2019), https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html [https://perma.cc/24EN-FDWC] ("The criminals strike up a conversation and gradually build trust. Often they pose as children, confiding in their victims with false stories of hardship or self-loathing. Their goal, typically, is to dupe children into sharing sexually explicit photos and videos of themselves—which they use as blackmail for more imagery, much of it increasingly graphic and violent.").

[123] *See* MONIQUE MATTEI FERRARO & EOGHAN CASEY, INVESTIGATION CHILD EXPLOITATION AND PORNOGRAPHY: THE INTERNET, THE LAW AND FORENSIC SCIENCE 46–47 (Mark Listewink et al. eds., 2005).

[124] DJ Mico, *Protecting the Digital Playgrounds: Narrowly Tailoring the Meaning of "Social Media" to Prohibit Sexual Predators from Using Social Media*, 51 U. PAC. L. REV 123, 125 (2019) ("Of approximately 6,000 reports of 'online enticement' across different social media and messaging applications, the most common methods offenders used to entice children included engaging in sexual conversation, asking children for sexually explicit images of themselves, and discussing interests or 'liking' the child's online posts to develop a rapport with the child.") (footnote omitted).

[125] *See* Saponaro v. Grindr, LLC, 93 F. Supp. 3d 319, 323 (D.N.J. 2015) (holding internet service provider was statutorily immune from liability in tort, pursuant to Communications Decency Act, for its alleged negligence in failing to monitor social networking site and allowing minor child to access site to arrange sexual encounter); Doe v. SexSearch.com, 551 F.3d 412, 415-16 (6th Cir. 2008) (dismissing several of plaintiff's claims against the website after underage user lied about her age, used the website, and engaged in sexual relations with the plaintiff); In re Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 295 (3d Cir. 2016) (holding that Google did not violate the Wiretap Act,

target young people that respond well to online attention, particularly those that are "insecure, needy, [and] isolated."[126] Children are apt to disclose personal information, either intentionally or unintentionally, thereby making a sexual predator's "grooming" that much easier.[127]

IV. PROPOSED ADJUSTMENTS

[32] Upcoming generations deserve protection from voracious data collectors. Several solutions have been offered.[128] Reevaluating the framework by which today's social media use and online activity is understood will hopefully contribute to the burgeoning scholarship about online privacy protection. As the previous section outlined, surveillance capitalism fundamentally alters the way we interact online and presents unprecedented problems for Generation Z—and beyond.[129] Thus, as

California Invasion of Privacy Act, New Jersey Computer Related Offenses Act, or Video Privacy Protection Act when it collected personal information about children).

[126] *How Predators Groom and Control their Victims*, FOCUS FOR HEALTH, https://www.focusforhealth.org/how-predators-groom-and-control-their-victims/.

[127] Dickson A. Abimbola-Akinola, The Cyber Crime and Internet and Internet Sexual Exploitation of Children" (Feb. 2017) (Student Thesis, Governors State University); *but cf.* Gehman, *supra* note 3, at 161–62 (arguing that children have a right to self-expression on social networking sites despite the infiltration of sexual predators).

[128] *See infra* text accompanying notes 137–39.

[129] *Compare* Joe Pinsker, *Oh No, They've Come Up With Another Generation Label*, THE ATLANTIC (Feb. 21, 2020), https://www.theatlantic.com/family/archive/2020/02/generation-after-gen-z-named-alpha/606862/ [https://perma.cc/LC6M-PPED] ("Generation Alpha . . . will grow up to be . . . the most technologically immersed [generation]."), *with* Brian Sharon (@ThatBShar), TWITTER (Mar. 19, 2020, 1:09 PM), https://twitter.com/ThatBShar/status/1240701836132155393 [https://perma.cc/A3G9-5HDB] ("There's so much video calling going on that the babies conceived during the coronavirus pandemic should be called 'Baby Zoomers'. @zoom_us"), *and* Kevin Smith (@KevinSmithNBA), TWITTER (Mar. 25, 2020, 7:23 PM), https://twitter.com/KeithSmithNBA/status/1242955200102629376 [https://perma.cc/B8HE-34EG] ("Are we all agreed that babies born 9 months after

COPPA enters its third decade, understanding the mechanisms of data collection becomes more pertinent.

A. Promulgation of COPPA

[33] As the number of internet-connected devices increases,[130] our concept of the internet will disappear.[131] The sprawl of our internet-connected and online-focused world highlights the need for increased protection for our children. COPPA must evolve with our increasingly connected world:

> [S]ince the enactment of COPPA, the internet has grown and the way data is stored, collected, and disseminated over the internet has become more complex and more prominent. '[I]n light of [these] changes in online technology,' the FTC amended the Rule in 2013 to 'clarify the scope of the Rule and strengthen its protections for children's personal information . . . .'[132] The amendment modified certain definitions, updated COPPA's requirements, and included a new provision regarding data retention and deletion. Despite these efforts to better align COPPA with the potential harms

COVID-19 are going to be call coronials? And in 2033/2034 they'll all become quaranteens? #dadjoke").

[130] *See generally* Peter M. Lefkowitz, *The Profession: Making Sense of the Internet of Things*, 59 BOSTON. B. J. 23 (2015) (examining the Internet of Things and how devices will grow in future years).

[131] *See* Dave Smith, *Google Chairman: 'The Internet Will Disappear'*, BUSINESS INSIDER (Jan. 25, 2015), https://www.businessinsider.com/google-chief-eric-schmidt-the-internet-will-disappear-2015-1 [https://perma.cc/S3SU-FHJ5] (quoting Google Chairman Eric Schmidt: "[T]he internet will disappear . . . . There will be so many IP addresses … so many devices, sensors, things that you are wearing, things that you are interacting with that you won't even sense it. It will be part of your presence all the time.").

[132] Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972 (Jan. 17, 2013) (codified at 16 C.F.R. pt. 312).

> child internet users face, the 2013 revision still falls short in meeting its stated goals of protecting children's internet privacy. Accordingly, the need to protect child privacy online remains strong and relevant.[133]

FTC Commissioner Noah Phillips opined:

> [T]he American privacy framework is built upon identifying risks and then designing a solution that balances competing interests. That requires evaluating the sensitivity of the information involved and the potential harms that would result from its collection, use or disclosure, and then creating a solution that will limit these harms while still allowing appropriate use of even sensitive information. With COPPA, rather than trying to protect children by limiting their experience on the Internet, Congress instead created a comprehensive, yet flexible, framework to protect both children's privacy and their ability to access interactive content on the Internet.[134]

[34] Before considering additional COPPA amendments, Commissioner Phillips stressed that original intent[135] must be remembered, rulemaking

---

[133] Shannon Finnegan, Note, *How Facebook Beat the Children's Online Privacy Protection Act: A Look into the Continued Ineffectiveness of COPPA And How to Hold Social Media Sites Accountable in the Future*, 50 SETON HALL L. REV. 827, 830 (2020) (footnotes omitted).

[134] Noah Joshua Phillips, Comm'r, Fed. Trade Comm'n Remarks at The Future of the COPPA Rule: FTC Staff Workshop, at 2 (Oct. 7, 2019), https://www.ftc.gov/public-statements/2019/10/remarks-commissioner-noah-joshua-phillips-ftc-workshop-future-coppa-rule [https://perma.cc/7MK4-B8TL].

[135] *See* 144 CONG. REC. S11, 657 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan) (stating COPPA's original goals: "to enhance parental involvement in children's online activities to protect both their privacy and safety; to maintain the security of the personally identifiable information collected from children online; and to protect

must be "grounded in facts, . . . rather than predicated on unsupported fear or speculation[,]" and regulation must focus on harmful conduct, not data collection in general.[136] Currently, there are several proposed solutions for online privacy issues that range from the imposition of a fiduciary duty on entities that collect or retain users' information[137] to banning sexual predators on social media[138] to shifting the regulation to state legislatures.[139]

B. COPPA's Limitations

[35] Several articles—coincidentally written by juris doctorate candidates—address the general inefficiency of COPPA and online privacy laws.[140] Perhaps the most notable problem is that kids frequently lie about

children's privacy by limiting the collection of personal information from children without their parent's consent.").

[136] Phillips, *supra* note 134, at 4–5.

[137] *See* Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893, 1929 (2019).

[138] *See* Mico, *supra* note 124.

[139] *See* Blaire Bayliss, *The Kids Are Alright* 😇 🍆 🍑*: Teen Sexting, Child Pornography Charges, and the Criminalization of Adolescent Sexuality*, 91 U. Colo. L. Rev. 251, 280–281 (2020).

[140] *See, e.g.*, Christie Dougherty, *Every Breath You Take, Every Move You Make, Facebook's Watching You: A Behavioral Economic Analysis of the US California Consumer Privacy Act and EU E-Privacy Regulation*, 12 NE. U. L. REV. 629, 658 (2020) ("Informed consent is meaningless in the area of privacy law when companies exploit consumers' irrational behaviors and inabilities to accurately and completely assess the tradeoffs of privacy disclosures."); Lauren A. Matecki, *Update: COPPA Is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era*, 5 NW. J.L. & SOC. POL'Y 369, 370 (2010); Mark Peasley, *It's Time for an American (Data Protection) Revolution*, 52 AKRON L. REV. 911, 943 (2018); Nicole Smith, *Protecting Consumers in the Age of the Internet of Things*, 93 ST. JOHN'S L. REV. 851, 866 (2019).

their age.[141] In 2011, a study found that about 40% of teens lie about their age to access a website or signup for an online account.[142] By 2014, another study found that one-quarter of U.S. children between the ages of 8 and 12 use Facebook.[143] Moreover, children are not the sole falsifiers: parents also help their children circumvent many age-restricted sites.[144]

[36] Websites set their minimum age to thirteen primarily because of COPPA's restriction. [145] Because websites are seemingly complaint, the

[141] *See* Madden et al., *supra* note 96.

[142] *Id.*

[143] Mary Aiken, *The Kids Who Lie About Their Age to Join Facebook*, THE ATL. (Aug. 30, 2016). https://www.theatlantic.com/technology/archive/2016/08/the-social-media-invisibles/497729/ [https://perma.cc/JXE7-X7AL] ("It wasn't just 11-to-12-year-olds who were going there: 34 percent of the Facebook users in the study were 8-to-10-year-olds. In the EU study, one-quarter of the 9-to-10-year-olds and one-half of the 11-to-12-year-olds were using the site as well: Four out of 10 gave a false age.").

[144] *See* Danah Boyd et al., *Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act'*, 16 FIRST MONDAY 11 (2011), https://journals.uic.edu/ojs/index.php/fm/article/download/3850/3075 [https://perma.cc/6T2X-BVZM] ("The online industry's response to COPPA's under–13 rule and verifiable parental consent model is largely proving incompatible, and at times, antithetical to many parents' ideas of how to help their children navigate the online world. Instead of providing more tools to help parents and their children make informed choices, industry responses to COPPA have neglected parental preferences and have altogether restricted what is available for children to access. As a result, many parents now knowingly allow or assist their children in circumventing age restrictions on general–purpose sites through lying. By creating this environment, COPPA inadvertently hampers the very population it seeks to assist and forces parents and children to forgo COPPA's protection and take greater risks in order to get access to the educational and communication sites they want to be part of their online experiences."); *accord* Steven Johnson, *The Bargain at the Heart of the Kid Internet*, THE ATL. (Apr. 12, 2018), https://www.theatlantic.com/family/archive/2018/04/child-data-privacy/557840/ [https://perma.cc/3GE5-V5GN].

[145] *See* Bethany Brown, Comment, *Children's Right to Privacy on the Internet in the Digital Age*, 20 J. TECH. L. & POL'Y 223, 225, 227 (2020) (stating that the Children's Online Privacy Protection Rule described anyone under the age of thirteen as a child).

FTC has had little incentive to reevaluate COPPA's restriction.[146] Consequently, the FTC has not challenged this process, effectively accepting that age disclosure with a minimum age requirement sufficiently complies with COPPA.[147]

[37] Enforcing these restrictions is also an issue.[148] "The vast ineffectiveness of COPPA, and the failure to adequately enforce it in a manner that promotes its underlying objectives, supports Zuckerberg's opinion that a law to regulate teenage data—if bearing any resemblance to COPPA—would likely be unnecessary."[149] COPPA's enforcement determines its effectiveness: the FTC must be properly equipped to enforce COPPA as legislators continue regulating the "Tech Titans."[150]

C. Modest Proposals

[38] In their review of *The Age of Surveillance Capitalism*, Justice Cuéllar and Professor Huq animadvert on how legal scholars disregard the ambiance of neoteric technology:

> [L]egal scholarship tends to be discrete in its focus and granular in its analysis when it comes to novel technological development. We myopically scrutinize a specific technology, such as social media platforms, machine

[146] Finnegan, *supra* note 133, at 835.

[147] Andrea M. Matwyshyn, *Of Teenagers and Tweenagers: Professor Allen's Critique of the Children's Online Privacy Protection Act in Historical Perspective*, 13 AM. PHIL. ASS'N NEWSL. 8 (2013) [hereinafter Matwyshyn, *Of Teenagers and Tweenagers*]; *see also* Andrea M. Matwyshyn, *Generation C: Childhood, Code and Creativity*, 87 NOTRE DAME L.R. 1979, 2018–2022 (2012) (arguing for the extension of the minority doctrine to digital spaces) [hereinafter Matwyshyn, *Generation C*].

[148] *See* Brown, *supra* note 145, at 227.

[149] Finnegan, *supra* note 133, at 828.

[150] *See id.*

> learning, or the internet of things, and try to understand how that phenomenon relates to existing legal templates. This work is valuable, even essential. But scholars and lawyers can miss the forest for the trees when they consider only parts rather than the integrated whole of the emerging data-driven economy. System-level effects, whether positive or negative, may be missed when discrete technologies or legal changes are analyzed in isolation. Gains or losses that spill over from one domain of human activity to another may be sliced out of the analytic frame. Without a clear sense of how discrete technologies are deployed, legal scholars are left with the feeling that they know something is happening, but they don't know what it is.[151]

[39] The issue has been framed, the stage set, the gauntlet laid. The following three proposals address the need for more consumer protection, especially for children, in hopes of advancing the privacy rights conversation. Given the gradual regulation of the internet's rapid metamorphosis, these proposals will undoubtedly contain overlooked—and possibly outdated[152]—issues in the coming months and years. However, the

[151] Mariano-Florentino Cuéllar & Aziz Z. Huq, *Economies of Surveillance*, 133 HARV. L. REV. 1280, 1283–84 (2020) (reviewing SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019)).

[152] *See, e.g.*, Euirim Choi, *Facebook Offers Money to Reel in TikTok Creators*, WALL ST. J., (July 28, 2020, 5:30 AM), https://www.wsj.com/articles/facebook-seeks-to-reel-in-tiktok-creators-raising-stakes-in-social-media-rivalry-11595928600 [https://perma.cc/4VW4-G8E6] (discussing Facebook's new service, Instagram Reels, which aims to compete with TikTok and is scheduled to launch in the U.S. and other countries in August 2020); Rob Copeland, *Google's Advertising Haul Comes Up Short for First Time*, WALL ST. J., (last updated July 30, 2020, 7:26 PM), https://www.wsj.com/articles/google-alphabet-googl-2q-earnings-report-2020-11596139328 [https://perma.cc/F5JF-CJXB] (noting Google's first quarterly revenue decline since its inception as a result of the global pandemic); Georgia Wells et.al., *Inside the Microsoft Talks to Buy TikTok's U.S. Business,* WALL ST. J., (last updated Aug. 3, 2020, 10:47 AM), https://www.wsj.com/articles/microsoft-aims-for-a-deal-to-buy-tiktoks-u-s-

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

1. Increase the Penalty

[40] Until the monetary penalties exceed the benefit of harboring children's behavioral data, companies will continue to violate COPPA. Until then, COPPA penalties will remain as another "cost of doing business."[153] Discovering the monetary value of children's online behavioral data is the main barrier from determining the appropriate penalty.[154] A framework shift from basic data collection to behavioral surplus is required to properly regulate these sites. Without austere 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."[155]

[41] As noted earlier, courts limit an operator's civil penalty to $43,280 per violation, though that amount decreases depending on several factors.[156] This amount is simply not enough to dissuade companies from collecting

business-11596418842 [https://perma.cc/E9GW-3T3V] (discussing the potential sale of TikTok to Microsoft in the coming weeks).

[153] *Cf.* Eldar Haber, *Toying with Privacy: Regulating the Internet of Toys*, 80 OHIO ST. L.J. 399, 441–442 (2019) ("[Online service provides] must not see fines as costs of doing business and should reflect further on the gravity of poor security measures. Policymakers should thus implant in the FTC more substantial regulatory teeth. This would enable the Commission's fines not merely to reflect the level of consumer loss but rather to sanction violations, with fines as percentages of annual global turnover.").

[154] *See, e.g.*, Noam Kolt, *Return on Data: Personalizing Consumer Guidance in Data Exchanges*, 38 YALE L. & POL'Y REV. 77, 87–88 (2020).

[155] ZUBOFF, *supra* note 73, at 105; *see also* TRACY, *supra* note 77. *See generally id.* at 104–105 (comparing Google and Facebook's unfettered freedom to Gilded Age "robber barons").

[156] *COPPA FAQs*, *supra* note 19.

children's data.[157] The FTC should raise the amount of each violation in substantial increments until the violations cease. Until the violations stop, the economic presumption is that the revenue generated from children's behavior is still higher than the cost of paying the penalty.[158]

2. Increase the Age

[42] COPPA's age minimum should be increased to eighteen.[159] As discussed earlier, the age of thirteen is arbitrary.[160] Common law recognizes the age of eighteen as the age of contractual capacity:

> [U]sing the age of thirteen as the ostensible age of consent for privacy contracting in digital spaces creates an irreconcilable conflict with the minority doctrine in contract law. Contract law has historically considered these concerns of child judgment when crafting its own rules. Since the

[157] In 2011, there were an estimated 7.5 million underage users on Facebook. Marc Perton, *Facebook's Zuckerberg wants to let kids under 13 onto site*, CONSUMER REPORTS NEWS (May 20, 2011), https://www.consumerreports.org/cro/news/2011/05/facebook-s-zuckerberg-wants-to-let-kids-under-13-onto-site/index.htm [https://perma.cc/33FE-TWE9]. As for a basic calculation: 7.5 million violations x $100-$43,280 penalty = $0.75-324.6 billion. Any increase in penalty would further—and possibly sufficiently—exacerbate a violator's punishment.

[158] Facebook's 2019 net income was over $18 billion and their 2019 Fourth Quarter net income was over $7 billion. Facebook Investor Relations, *Facebook Reports Fourth Quarter and Full Year 2019 Results*, FACEBOOK (Jan. 29, 2020), https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Fourth-Quarter-and-Full-Year-2019-Results/default.aspx [https://perma.cc/Q3VS-QEZ9]. Leaving the law-students-are-bad-at-math joke behind, Facebook could pay its "unprecedented" $5 billion settlement from its Q4 net income and still profit over $2 billion—just for that quarter!

[159] *Cf.* Berin Szoka & Adam Thierer, *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*, 16 PROGRESS & FREEDOM FOUND., at 6 n.20 (June 2009) (discussing the term "child" as someone under eighteen).

[160] Matwyshyn, *Of Teenagers and Tweenagers*, *supra* note 147 at 7.

> issue that COPPA . . . address[es] relates to a particular contracting context—data privacy and information security contracting—a logical age of consent is one which mirrors contractual capacity generally. Applying a contract law analysis, the usual age of contractual capacity is eighteen, not thirteen.[161]

[43] Moreover, there is a reason that children cannot vote,[162] enlist in the military,[163] drive,[164] consume tobacco,[165] drink alcohol,[166] or do several other activities:[167] a child's capacity to understand consequences develops with time. As such, companies should not exploit children's behavioral data until children have

[161] *Id.* at 8; *see also* Matwyshyn, *Generation C*, *supra* note 147.

[162] *See* Tex. Const. art. VI, § 1 (limited to eighteen and older).

[163] *See* TEX. GOV'T CODE ANN. § 437.302(b)(3) (West 2020) (eighteen and older).

[164] *See* TEX. TRANSP. CODE ANN. § 521.204(a)(1) (West 2020) (sixteen or older); TEX. TRANSP. CODE ANN. § 521.222 (West 2020) (learner's permit at age fifteen).

[165] *See* TEX. HEALTH & SAFETY CODE ANN. §§ 161.251–161.257 (West 2020) (twenty-one and older).

[166] *See* TEX. ALCO. BEV. CODE ANN. § 106.01–106.02 (West 2020) (twenty-one and older).

[167] *See, e.g.*, TEX. LABOR CODE ANN. § 51.011 (West 2020) (limiting employment to at least fourteen years of age); TEX. ALCO. BEV. CODE ANN. § 106.09(a) (West 2020) ("[N]o person may employ a person under 18 years of age to sell, prepare, serve, or otherwise handle liquor, or to assist in doing so."); TEX. LABOR CODE ANN. § 51.016(b) (West 2020) (limiting "sexual oriented employment" to at least eighteen years of age); TEX. PENAL CODE ANN. § 43.24(a–b) (West 2020) (prohibiting the sale or distribution of sexual material to a person younger than eighteen years of age); TEX. CIV. PRAC. & REM. CODE ANN. § 129.001 (West 2020) ("The age of majority in this state is 18 years."); TEX. ELEC. CODE ANN. § 141.001(a)(2) (West 2020) (limiting eligibility to run for public office to at least eighteen years of age).

turned eighteen. Adults can protect themselves from online manipulation,[168] but society must protect children.

3. Increase the Stakes

[44] The manufacturing of "prediction products" from children's behavioral data should be criminalized as another form of child abuse.[169] In the seminal case, *Packingham v. North Carolina*, the U.S. Supreme Court ruled on a state's law regulating social media sites for the first time.[170] There, the Court held that a North Carolina law prohibiting registered sex offenders from accessing a "commercial social networking Web site"[171] was too broad and thereby violated the First Amendment.[172] 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.[173]

[168] *Cf.* Johnson, *supra* note 92, at 447 (arguing that COPPA should extend to adults as well: "If COPPA applied across the board, companies, regulators, and the public would not need to engage in any exercises to determine whether COPPA applied. It would apply.").

[169] *See generally* 18 U.S.C. § 2252 (2018) (listing prohibited products involving minors).

[170] *See* Packingham v. North Carolina, 137 S. Ct. 1730 (2017).

[171] *See* N.C. GEN. STAT. ANN. §§ 14–202.5(a), (e) (2015).

[172] *See Packingham*, 137 S. Ct. at 1738.

[173] *Id.* at 1736.

[45] The Court further observed that all new technologies, including the internet and social media, will be "exploited by the criminal mind" and "become instruments used to commit serious crimes."[174] 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.[175]

[46] 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.[176] 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.[177]

[47] Legislators cannot adequately regulate the "new logic of accumulation" without understanding how online behavioral data are manipulated into "prediction products."[178] There is already a duty to report any online activity that sexually exploits children.[179] Buying and selling a child's online behavioral data is a short slip away from outright child exploitation.[180] The moral disparity between *offline* child exploitation and *online* child exploitation should be rectified.

---

[174] *Id.*

[175] *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.")

[176] *See id.* at 1739 (Alito, J., concurring).

[177] *Id.* at 1740 (Alito, J., concurring).

[178] *See* Shoshana Zuboff, *Surveillance Capitalism and the Challenge of Collective Action*, 28 NEW LAB. F. 10, 16 (2019).

[179] *See* 18 U.S.C. § 2258A(a) (2018).

[180] *Cf.* 15 U.S.C. § 6502 (2018) (requiring website operators to provide notice and obtain parental consent before collecting personal information from a child).

D. Current Exemplar

[48] The California Consumer Privacy Act (CCPA) is a current exemplar for how governments should respond to the ascension of surveillance capitalism.[181] California recently passed the CCPA to curtail rampant privacy violations online.[182] 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.[183] Furthermore, the CCPA allows the consumer to opt-out of having such personal information sold to third-parties.[184]

[49] Several key rights are established and protected by CCPA: (1) the right to know what personal information is obtained by companies, (2) the right to delete information companies obtain, (3) the ability to opt out from the sale of their personal information, and (4) the promise that consumers

[181] The EU General Data Protection Regulation (GDPR) is also another exemplar for regulating personal data and online privacy rights. *See* Jacob M. Victor, Comment, *The EU General Data Protection Regulation: Toward A Property Regime For Protecting Data Privacy*, 123 YALE L. J. 513, 513–14 (2013) (discussing the GDPR's background and proposed regulations); *What is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ [https://perma.cc/3UEF-FRW3].

[182] *See* CAL. CIV. CODE § 1798.100 (West 2020); Practical Law Data Privacy Advisor, *Understanding the California Consumer Privacy Act (CCPA)*, WESTLAW (2020); *see also* John Stephens, *California Consumer Privacy Act*, ABA (Feb. 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/#:~:text=The%20California%20Consumer%20Privacy%20Act%20of%202018%20was%20approved%20by,effect%20on%20January%201%2C%202020.&text=This%20prompted%20the%20California%20legislature,control%20of%20their%20personal%20information [https://perma.cc/A3W4-2KNQ] (discussing background and history of the CCPA); Dominique-Chantale Alepin, *Social Media, Right To Privacy And The California Consumer Privacy Act*, 29 J. ANTI., UCL & PRIV. SEC. CAL. ASSOC. 96, 96 (2019); *Your Data Is Shared and. Sold…What's Being Done About It?*, UNIV. OF PA. (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ [https://perma.cc/5AFP-BR98].

[183] *See* CAL CIV. CODE § 1798.110 (Deering 2020).

[184] *See* CAL CIV. CODE § 1798.120 (Deering 2020).

will not be discriminated against for following through with any of these options.[185] Finally, "express authorization" is required for a minor consumer's personal information to be sold.[186] Given the novelty of this legislation, case law has not clarified what "express authorization" requires.[187]

V. CONCLUSION

[50] These times are certainly a-changin'. Privacy concerns are at the forefront of the internet's proliferation. Behemoths like Facebook and Google are leading the way into the digital frontier, and FTC penalties are metaphorical drops in the bucket on their path to malapert achievements. Privacy is no longer a give-and-take scenario: companies freely take all we have and leave us with apps to update and newsfeeds to scroll. Future research will soon point to the irrelevancy of this paper's diminished understanding of the internet today. This latency only shows the speed at which the internet transforms our world. Nevertheless, these issues must be discussed for the conversation to continue.

---

[185] Lauren Davis, *The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation*, 24 N.C. BANKING INST. 499, 505–07 (2020) (discussing the right to know, right to be forgotten, right to opt out, and the right to equal service and pride); *see, e.g.*, John W. Dowdell, Comment, *An American Right to be Forgotten*, 52 TULSA L. REV. 311, 321 (2017) ("The right to be forgotten – the most controversial proposal by any measure – was described by the European Commission as 'the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes.'").

[186] *See* CAL CIV. CODE § 1798.120 (Deering 2020); CAL CIV. CODE § 1798.135 (Deering 2020).

[187] *Cf. Express*, BLACK'S LAW DICTIONARY (11th ed. 2019) (defining express as "[c]learly and unmistakably communicated; stated with directness and clarity."); *Authorization*, BLACK'S LAW DICTIONARY (11th ed. 2019) (defining authorization as the "[o]fficial permission to do something" or "[t]he official document granting such permission."); FACEBOOK, https://www.facebook.com/help/contact/784491318687824 [https://perma.cc/9HHR-ZPSR] (displaying a form that Facebook and Instagram have that allows California residents to exercise their rights under the CCPA).

[51] Come Senators, Congresspeople, please heed the call. A child's life has value and deserves protection. Children are already functioning as consumers and will soon enter the "real world" knowing no other lives aside from their screens. Leaders are made for the occasion as much as the occasion is made for leaders. Children must be protected as society begins surveying the frontier of surveillance capitalism.