COPPA AS CATALYST: RECALIBRATING THE FTC'S PRIVACY ENFORCEMENT FRAMEWORK

*Michael W. Berg**

ABSTRACT

While there is no federal legislation protecting digital privacy generally, there are industry- or population-specific statutes that empower federal agencies to police data usage among businesses. The Children's Online Privacy Protection Act of 1998 is one such statute: it empowers the Federal Trade Commission to publish regulations pertaining to children's privacy and enforce those regulations with legal action. The most recent such regulation was promulgated in 2013; given the enormous changes in technology since then, the agency would be well-advised to revisit its framework for enforcing COPPA. This Note will offer suggestions for providing more robust regulations that better reflect the modern digital landscape, including both a "negative" framework involving a more transparent and strict penalty scheme and a "positive" framework providing a safe harbor for regulated entities. In addition, this Note will advocate for the agency to leverage parental concern and engage with state legislatures to further protect underaged internet users.

TABLE OF CONTENTS

INTRODUCTION 1012
I. DATA PRIVACY AND THE LAW 1014
A. *The State of the Internet* 1015
B. *Privacy Enforcement at the FTC* 1018
II. PROTECTING CHILDREN'S PRIVACY: HISTORY AND CURRENT STATUS 1020
A. *Passing COPPA* 1020
B. *FTC Enforcement of COPPA* 1023

* The author would like to extend his gratitude to the inimitable Prof. Steve Gold for his guidance (and patience!) throughout the process of writing this Note, and to his wife, Joan Brittingham, for her endless and ferocious support throughout the law school experience.

III. PROPOSED POLICY CHANGES 1026
A. *Rethinking COPPA Enforcement at the FTC* 1027
1. Positive Federal Protection: Adjusting Expectations 1027
2. Negative Federal Protection: Recalibrating the Penalties 1030
B. *Leveraging Privacy from the Ground Up* 1033
1. Encouraging Parental Involvement 1034
2. Encouraging the Growth of "Super-Regulators" 1035
CONCLUSION 1040

INTRODUCTION

Since its conception in the 1960s, the distributed network of servers known as "the internet" has evolved from an academic exercise into a high-end tool for specialized technology vendors and users, then into an entertaining and lucrative collection of consumer activities, and most recently into a pervasive facet of daily life for most people living in the United States.[1] Like electricity or indoor plumbing, "internet access" has become a given, perhaps even a necessity: we assume that we will be able to search for an answer to any possible question, connect with far-flung friends and family, and access a wide range of entertainment options at almost any point in our daily lives.[2]

---

1. *See generally, e.g.*, ANDREW PERRIN & MAEVE DUGGAN, AMERICANS' INTERNET ACCESS: 2000-2015 (2015), https://www.pewresearch.org/internet/2015/06/26/americans-internet-access-2000-2015/.

2. Many believe that internet access has become so fundamental to participation in the modern economic system that it constitutes an essential human right. *See, e.g.*, Jack J. Barry, *COVID-19 Exposes Why Access to the Internet Is a Human Right*, OPENGLOBALRIGHTS (May 26, 2020), https://www.openglobalrights.org/covid-19-exposes-why-access-to-internet-is-human-right/. *But see* Vinton G. Cerf, *Internet Access Is Not a Human Right*, N.Y. TIMES (Jan. 4, 2012), https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html; Michael O'Rielly, Comm'r, Fed. Commc'ns Comm'n, Remarks Before the Internet Innovation Alliance:
What Is the Appropriate Role for Regulators in an Expanding Broadband Economy? (June 25, 2015), https://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0625/DOC-334113A1.pdf.

While not going quite so far as to label internet access a fundamental right, the United Nations released a report in 2011 noting that, given the "key role that the Internet can play in mobilizing [residents of any given nation] to call for justice, equality, accountability and better respect for human rights[,] . . . facilitating access to the Internet for all individuals . . . should be a priority for all States." Frank La Rue (Special Rapporteur), Hum. Rts. Council, *Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*,

But this tool, flexible and powerful as it is, comes with concerns, particularly regarding privacy. Most developers of internet-based applications are happy to share their products with consumers at no direct cost; instead, consumers pay a cost in privacy as developers use the features of their apps, programs, and pages to harvest data, including browsing habits, purchasing predilections, political leanings, and geographical locations, a phenomenon some describe as "surveillance capitalism."[3] Legislatures and government agencies both in the United States and abroad have established legal protections that attempt to address these practices, whether by restraining the data-mining that powers this economic ecosystem, identifying and regulating entities that purchase and use this data, empowering consumers to have a say in how their data is harvested and collected, or any combination thereof.[4]

Children and adolescents are generally recognized to be particularly vulnerable in the digital sphere.[5] Recognizing this, Congress passed the Children's Online Privacy Protection Act ("COPPA") in 1998, empowering the Federal Trade Commission ("FTC") to establish a regulatory regime to set standards for businesses that develop online content for children and adolescents and hold them accountable for failing to comply with those standards.[6] While the agency's enforcement

---

U.N. Doc. A/HRC/17/27, at 4 (May 16, 2011), https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

3. *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019). Zuboff asserts that the shift to a digital marketplace and the accompanying marketability of consumer data represents a fundamental shift in economic structure, akin to such historic trends as the creation of the assembly line and the commodification of labor. *Id.* at 85–87, 98–100. In their review of the book, Mariano-Florentino Cuéllar and Aziz Z. Huq dispute the scale of Zuboff's claim, arguing that "surveillance capitalism" (as they term it) represents a logical outgrowth of twentieth-century industrialization practices. Mariano-Florentino Cuéllar & Aziz Z. Huq, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. By Shoshana Zuboff*, 133 HARV. L. REV. 1280, 1295–97 (2020) (book review). While Cuéllar and Huq push back on some of Zuboff's more alarmist tendencies, they agree that the novel political, economic, and social realities created by this trend have troubling aspects and that the legal system has a responsibility to intercede to protect internet users from the resulting concentrations of power that may form. *Id.* at 1335–36.

4. *See, e.g.*, Anupam Chander et al., *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1734–36 (2021).

5. *See, e.g.*, Wouter M. P. Steijn & Anton Vedder, *Privacy Under Construction: A Developmental Perspective on Privacy Perception*, 40 SCI., TECH., & HUM. VALUES 615, 616–18 (2015).

6. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506. The FTC, as directed by this statute, promulgated a rule outlining the scope of its authority; the requirements for notice, consent, and review; various safeguards, prohibitions, and requirements; and its general enforcement posture. Children's Online Privacy Protection Rule, 64 Fed. Reg. 22750 (Apr. 27, 1999) (to be codified at 16 C.F.R. pt. 312). For an in-depth review of the statute, the FTC's understanding of its authority under it, and concerns

efforts have not been lacking, there is ample evidence suggesting that the current enforcement structure should be recalibrated to meet the needs of a vastly different internet than was available either at the time of the statute's passage or as of the most recent regulatory update published by the agency in 2013.[7]

This Note will offer options for adjusting COPPA enforcement to both provide a stronger deterrent to bad actors and more accurately reflect the modern landscape of internet usage and data exploitation. Part I will describe the current state of data privacy, particularly for underaged internet users, and include a brief summary of the FTC's history as a protector of consumer privacy. Part II will describe the passage of the statute itself, detail the agency's regulatory posture, and evaluate recent trends in COPPA enforcement as well as evidence of growing concerns from stakeholders. Part III will offer some potential routes that the FTC could take to adjust its enforcement practices.

These suggestions will begin with regulatory steps the agency should consider, including a "safe-harbor" privacy notification provision and a more transparent and stringent penalty regime for violating privacy requirements. While the penalty regime will need to be tailored to the needs of the digital marketplace, the primary structure for the proposed framework is borrowed from the "benefit and gravity" scheme employed by the FTC's sister agency, the Environmental Protection Agency ("EPA"). To complement these regulatory measures, this Note will then suggest that the agency engage in education and advocacy at the local and state levels by encouraging parents to advocate for their children's privacy and working with state legislatures to increase state-level statutes in a manner that creates a network of "super-regulators" protecting digital privacy.

I. DATA PRIVACY AND THE LAW

Since the earliest days of the consumer-driven internet, there have been concerns about protecting the data that people (both adults and children) generate through online activity.[8] These concerns have evolved

---

regarding privacy regulation and underaged users in general, see CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 193–215 (2016).

7. *See generally* 16 C.F.R. § 312 (2013). After requesting public input via the Federal Register, the agency "received over 350 comments in response." Children's Online Privacy Protection Rule, 64 Fed. Reg. 3972, 3973 (Jan. 17, 2013) (to be codified at 16 C.F.R. pt. 312). The resulting rule "modif[ied] the definitions of both *operator* and *Web site or online service directed to children*" for several reasons, chief among them to clarify the responsibilities of third parties (e.g., plug-in creators and advertising entities) under the statute. *Id.*

8. *See* HOOFNAGLE, *supra* note 6, at 145, 193.

along with the internet itself, and the FTC has frequently found itself at the nexus of these concerns.

A. *The State of the Internet*

The internet as it exists today is the result of decades of research and development.[9] Computer scientists began developing computer networking systems as early as the 1960s, and Ray Tomlinson wrote the first successful email application in 1972.[10] These early efforts gave rise to the internet of today, a decentralized network of servers utilizing a system of globally unique addresses based on common protocols for transmitting and retaining information.[11] At first, large-scale industrial entities were the primary users of this new technology; it was not until the 1990s that domestic use of the internet became widely available.[12] As such use became more widespread, the economic framework of the internet as a whole came into question: what would the primary funding sources be for this increasingly popular tool?

The answer split along an "infrastructure v. content" fault line. In the first instance, consumers paid for access to the internet in general via an ever-broadening selection of internet service providers ("ISPs"), primarily consisting of existing telephone and cable companies seeking to bundle internet access into existing service plans.[13] Content providers, however, found it difficult to convince consumers to pay directly to access their services, and instead pivoted to providing "free" content that generated income by selling advertising space.[14] As this practice grew, software developers began to tap into user-provided information in order

---

9. Barry M. Leiner et al., *A Brief History of the Internet*, 39 COMPUT. COMMC'N REV. 22, 22 (2009).

10. *Id.* at 23–24.

11. *Id.* at 30.

12. *Id.* at 26, 30–31.

13. *See* EV EHRLICH, A BRIEF HISTORY OF INTERNET REGULATION 8–9 (2014), https://www.progressivepolicy.org/wp-content/uploads/2014/03/2014.03-Ehrlich_A-Brief-History-of-Internet-Regulation1.pdf; *see also* Jane Reuter, *A Brief History of Internet Service Providers*, VIASAT: SATELLITE INTERNET BLOG (Aug. 13, 2019, 12:00 AM), https://www.viasat.com/about/newsroom/blog/a-brief-history-of-internet-service-providers/; *see also* Jeffrey A. Hart et al., *The Building of the Internet: Implications for the Future of Broadband Networks*, 16 TELECOMMS. POL'Y 666, 688 (1992) (explaining some of the technical issues facing both broadband and telephone companies in the initial struggles for the burgeoning internet service provider market).

14. *See* Brian X. Chen, *The Battle for Digital Privacy Is Reshaping the Internet*, N.Y. TIMES (Sept. 21, 2021), https://www.nytimes.com/2021/09/16/technology/digital-privacy.html. Interestingly, Chen also points out that public concern about privacy has led to a resurgence of subscription-based content access. *Id.* This could prove disruptive in the long term: "[i]f personal information is no longer the currency that people give for online content and services, something else must take its place." *Id.*

to create extremely detailed accounts of individual user activity that could then be used to develop targeted advertising protocols based on each user's browser and purchase history.[15]

Over the past twenty years, both the available reach of data and the scope of potential uses for this data have grown drastically. The advent of smartphones gave data harvesting entities the ability to collect geographical data on their users' movements.[16] Social media outlets provided insights into large-scale behavioral traits, ranging from entertainment preferences such as literary or popular culture "fandoms" to political or religious affiliations.[17] As the scope of available data grew, so too did the use to which it could be put; advertising based on digital surveillance remained commonplace, of course, but purchasing data on potential new hires or renters became relatively common practices among employers or landlords, respectively.[18]

Public awareness of commercialized uses of personal data has increased in the last few years, and with it pressure for regulators to restrain both data-harvesting and -selling practices.[19] In the United States, the legal landscape surrounding digital privacy is a patchwork.[20] Surprisingly, although the internet is both ubiquitous and borderless, Congress has made no laws aimed at providing holistic protections for digital privacy writ large.[21] Instead, many state legislatures have enacted their own privacy standards, some of which form a baseline of

15. *See* APRIL FALCON DOSS, CYBER PRIVACY: WHO HAS YOUR DATA AND WHY YOU SHOULD CARE 59–63 (2020); *see also* ZUBOFF, *supra* note 3.

16. *See, e.g.*, Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN STATE L. REV. 777, 783–84 (2016); *see also* DOSS, *supra* note 15, at 208–10, 224; Mary Beth Quirk, *Study: Some Popular Android Apps Tracking User Location Once Every Three Minutes*, CONSUMERIST (Mar. 24, 2015, 4:12 PM), http://consumerist.com/2015/03/24/study-some-popular-android-apps-tracking-user-location-once-every-three-minutes/.

17. *See* DOSS, *supra* note 15, at 65–68.

18. Cuéllar & Huq, *supra* note 3, at 1290–91. Governmental use of personal data is outside the scope of this Note but is a significant concern as well. For more information on the ways in which government entities utilize personal data in pursuit of goals, such as national security, criminal investigation and prosecution, etc., see April Falcon Doss, *Data Privacy & National Security: A Rubik's Cube of Challenges and Opportunities That are Inextricably Linked*, 59 DUQ. L. REV. 231, 235–36 (2021). *See also* Cuéllar & Huq, *supra* note 3, at 1326–31 (emphasizing "both the peril and the promise of a 'surveillance state' as both aspiring political monopolist and potential regulator").

19. Chen, *supra* note 14.

20. *See* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

21. *See id.*

common practice among digital content providers.[22] Their efforts have led to some broad shifts in issues of digital privacy, as content creators have chosen to adopt "one-size-fits-all" approaches to statutory compliance rather than invest in multilayered, geographically based privacy policies.[23]

This is not to say, of course, that Congress has not addressed digital privacy at all.[24] Rather, they have declined to do so in any sweeping fashion, instead choosing to pass piecemeal legislation targeted at specific sectors of American life.[25] For instance, the Health Insurance Portability and Accountability Act ("HIPAA") and the Gramm-Leach-Bliley Act ("GLBA") focus on the medical and financial industries respectively and task the Department of Health and Human Services ("HHS") and the FTC with enforcement.[26] COPPA is one such statute, focused on a population group (children aged thirteen and younger) rather than a sector of industry.[27]

Unfortunately, congressional action along the digital frontier has been lacking in recent years.[28] Debates about net neutrality and regulations for social media giants have dominated the technological discussion at the congressional level; through these conversations, legislators have demonstrated an embarrassing lack of knowledge about digital technology in general and about how internet-based entities such as Google and Facebook collect, package, and sell information in particular.[29] In contrast, the FTC has thankfully demonstrated a

22. *See, e.g.*, Chander et al., *supra* note 4, at 1738–89 (outlining the fragmented nature of privacy regulation, both within the United States and worldwide). One statute in particular—the California Consumer Privacy Act ("CCPA")—is particularly important and will be discussed in more depth *infra* Section III.B alongside the legal efforts of the European Union. Together, these two entities have provided the most serious legal protections of digital privacy, but there is still ample space for the FTC to play a role in shaping and clarifying privacy interests and industry standards in a way that promotes a better-informed and healthier dialogue between providers and consumers.

23. *See infra* Section III.B.2.

24. *See, e.g.*, Klosowski, *supra* note 20.

25. *See id.*

26. Anupam Chander et al., *Achieving Privacy*, 74 SMU L. REV. 607, 613–14 (2021).

27. *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.

28. *See* Klosowski, *supra* note 20.

29. Examples of such embarrassment abound. One of the most memorable instances of this phenomenon occurred during a Senate committee hearing on net neutrality in 2006, when Senator Ted Stevens (R-AK) opined that the internet was "a series of tubes." Ken Belson, *Senator's Slip of the Tongue Keeps on Truckin' Over the Web*, N.Y. TIMES (July 17, 2006), https://www.nytimes.com/2006/07/17/business/media/17stevens.html. *But see* Evan Dashevsky, *A Remembrance and Defense of Ted Stevens' 'Series of Tubes'*, PCMAG (June 5, 2014), https://www.pcmag.com/news/a-remembrance-and-defense-of-ted-stevens-series-of-tubes.

relatively high level of competence overall, particularly in its recent demands for wide-ranging information about industry practices pertaining to data collection and usage in order to better inform its regulatory practices.[30]

B. Privacy Enforcement at the FTC

The Federal Trade Commission is one of the oldest federal agencies in existence, and it has one of the broadest mandates.[31] Originally created in 1914, the agency exists to protect consumers from unfair business practices; this includes everything from pursuing antitrust litigation to investigating and prosecuting instances of fraudulent, deceptive, or unfair marketplace practices.[32] Courts have traditionally

---

More recently, legislators have come under fire for not understanding this crucial component of modern life, whether in terms of social media, net neutrality, or online piracy. *See, e.g.*, Morgan Wright, *Congress is Clueless About Facebook — and That Should Make Us Panic*, HILL (Apr. 12, 2018, 6:45 AM), https://thehill.com/opinion/technology/382792-congress-is-clueless-about-facebook-and-that-should-make-us-panic; Devin Coldewey, *Congress Flaunts Its Ignorance in House Hearing on Net Neutrality*, TECHCRUNCH (Feb. 7, 2019, 4:26 PM), https://techcrunch.com/2019/02/07/congress-flaunts-its-ignorance-in-house-hearing-on-net-neutrality/; Catherine Rampell, *Our Politicians Have No Idea How the Internet Works*, WASH. POST (Aug. 20, 2018, 8:10 PM), https://www.washingtonpost.com/opinions/how-can-congress-police-the-internet-when-they-dont-even-understand-it/2018/08/20/46f6baa6-a4b4-11e8-97ce-cc9042272f07_story.html. Prior to the 104th Congress beginning its term in 1995, the Office of Technology Assessment ("OTA") existed to provide Congress with "impartial analysis of technology and science issues," but this agency was targeted for dissolution by the new Republican majority as part of its bid to decrease the size of government. *See* Darrell M. West, *It Is Time to Restore the US Office of Technology Assessment*, BROOKINGS INST. (Feb. 10, 2021), https://www.brookings.edu/research/it-is-time-to-restore-the-us-office-of-technology-assessment/. As the technology sector continues to grow, it remains to be seen whether Congress will heed Mr. West's advice and recreate the OTA to provide such impartial analysis once more.

30. The FTC got an early start in monitoring the activities of internet content providers, bringing its first case regarding internet use by consumers in 1994 and issuing policy statements as early as 1995. *See* HOOFNAGLE, *supra* note 6, at 145; *see also infra* Part II. For a look at how this expertise plays out in the context of enforcement, see generally April Falcon Doss, *December Brought Harbingers of the Regulation Social Media Companies Could Soon Face*, JUST SEC. (Jan. 12, 2021), https://www.justsecurity.org/74067/december-brought-harbingers-of-the-regulation-social-media-companies-could-soon-face/.

It is worth noting that many scholars argue that a more holistic federal approach is appropriate given the pervasiveness and power of the economic sphere based on this type of surveillance. *See generally* Doss, *supra* note 18; ZUBOFF, *supra* note 3. However, such large-scale congressional action seems unlikely in the near future. *See* discussion *infra* Section III.A.1.

31. For a full history of the agency, see generally HOOFNAGLE, *supra* note 6, at 3–81. For a compressed timeline, see *id.* at 11.

32. 15 U.S.C. § 45(a)(2) ("The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or

given the agency broad latitude to define these terms,[33] which the agency has done by publishing "statements of definition" and then targeting particularly egregious violations of these regulatory statements.[34] This enforcement pattern can best be described as a "quasi-common-law" approach that uses subsequent adjudications as the primary substantive method of detailing the specific contours of their broad-stroke rulemaking.[35]

Within this enforcement context, the FTC began monitoring online businesses for practices related to abuse of consumer privacy under the unfair and deceptive conceptual umbrellas as internet-based businesses grew more prevalent in the 1990s.[36] This was due to mounting pressure from consumer groups and Congress alike for the agency to take an active stance in addressing the potential dangers of the newly popular tool, particularly since European legislation promised to make things more difficult for American online businesses without firmer protections in place.[37] While the agency proceeded (albeit cautiously) with its traditional "common law" approach,[38] it also capitalized on this public

---

affecting commerce and unfair or deceptive acts or practices in or affecting commerce."); *see also* HOOFNAGLE, *supra* note 6, at 119.

33. *See, e.g.*, FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 239 (1972) (alteration in original) ("First, does s 5 [of the Federal Trade Commission Act] empower the Commission to define and proscribe an unfair competitive practice, even though the practice does not infringe either the letter or the spirit of the antitrust laws? Second, does s 5 empower the Commission to proscribe practices as unfair or deceptive in their effect upon consumers regardless of their nature or quality as competitive practices or their effect on competition? We think the statute, its legislative history, and prior cases compel an affirmative answer to both questions."). In the realm of privacy more generally, this has led to agency publications that focus on helping businesses achieve compliance with a broad range of privacy-related regulations. *See, e.g.*, *Consumer Privacy*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/consumer-privacy (last visited Mar. 13, 2023).

34. *See, e.g.*, *FTC Policy Statement on Unfairness*, FED. TRADE COMM'N (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness. Congress codified and amended this statement in 1994, focusing the "unfairness" inquiry on unjustified consumer injury. *See also* HOOFNAGLE, *supra* note 6, at 131.

35. *See, e.g.*, HOOFNAGLE, *supra* note 6, at 343–44 (discussing the agency's "common-law" approach in light of its freedom from some traditional common-law restrictions).

36. *See id.* at 156–66. Originally, agency officials believed that "unfairness as a legal theory did not fit the privacy practices of online services." *Id.* at 156 (citing Interview with Joan Z. Bernstein, Oral Hist. Project, The Hist. Soc'y of the D.C. Cir. (2007)). However, the agency's stance toward unfairness shifted in 2003 as it began to encounter online business practices that met the "substantial injury" requirement, such as changing privacy policies without or with minimal notice. *See id.* at 160–61.

37. *See id.* at 157.

38. *See id.* at 156–58. This process accelerated as the agency both developed more expertise with the technological aspects of the internet and grew an impressive body of legal precedent largely in the form of consent decrees. *See, e.g.*, Chander et al., *supra* note 26, at

pressure to encourage Congress to provide a statutory tool for protecting underaged internet users.[39]

II. PROTECTING CHILDREN'S PRIVACY: HISTORY AND CURRENT STATUS

The framework for protecting children's privacy is somewhat outdated compared to trends in online activity.[40] In recent years, however, private parties, states, and the FTC have all sought to protect the interests of underaged internet users using the COPPA toolbox, with varying degrees of success.[41] This Part details the passage of the original statute and describes various attempts to protect children's online privacy in order to set the scene for the proposed adjustments to the agency's COPPA enforcement regime in the final Part.

A. Passing COPPA

In the late 1990s, parents across the United States noticed with growing concern that children and adolescents were using the internet with increasing regularity and proficiency and that web-based businesses seemed to know more and more about their children.[42] These fears bore fruit as researchers and journalists discovered that large-scale data brokerage and marketing interests had developed extensive methods to target young people online and were willing to sell the data they retrieved from underaged users with little to no concern for either safety or privacy.[43]

---

613 (citing Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585–86 (2014)).

39. *See* HOOFNAGLE, *supra* note 6, at 157.

40. *See, e.g.*, SONIA LIVINGSTONE ET AL., CHILDREN'S DATA AND PRIVACY ONLINE: GROWING UP IN A DIGITAL AGE 3–4 (2018), https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf.

41. *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Strengthens Kids' Privacy, Gives Parents Greater Control over Their Information by Amending Childrens Online Privacy Protection Rule (Dec. 19, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over-their-information-amending-childrens.

42. *See, e.g.*, HOOFNAGLE, *supra* note 6, at 193.

43. *See, e.g.*, Press Release, Elec. Priv. Info. Ctr., Largest Database Marketing Firm Sends Phone Numbers, Addresses of 5,000 Families with Kids to TV Reporter Using Name of Child Killer (May 13, 1996) (on file with author). *But see* Ian C. Grant, *Young Peoples' Relationships with Online Marketing Practices: An Intrusion Too Far?*, 21 J. MKTG. MGMT. 607, 616–19 (2005) (detailing various ways in which advertisers experience "a lack of engagement" thanks to a combination of "highly insensitive targeting by marketing practitioners" and distrust resulting from "the increasingly blurred boundaries between commercial advertising and . . . content provision").

At the urging of the Center for Media Education ("CME"), the FTC investigated a website known as "KidsCom," a site that required children to provide extensive personal information in order to sign up and then leveraged that information to encourage children to spend intra-site virtual money ("KidsCash") on digital versions of well-known products.[44] While the agency did not take direct enforcement action against KidsCom,[45] its findings led the FTC staff and the White House to request that Congress take legislative action to grant the FTC explicit powers to enforce privacy standards for websites aimed at underaged users.[46] Congress soon granted this request by passing COPPA in 1998; it was the first federal statute dealing explicitly with online privacy.[47]

Through COPPA, Congress gave authority to both state governments and to the FTC to regulate entities that collect online data from children.[48] Such entities are only allowed to collect data from children with parental consent.[49] In addition, regulated entities must follow strict

---

44. *See* HOOFNAGLE, *supra* note 6, at 197.

45. *See id.* The reluctance to do so stemmed largely from the hesitance of agency staff to apply the "unfairness" doctrine to online businesses. *See supra* Section I.B; *see also* sources cited *supra* note 34.

46. *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 42–43 (1998); Press Release, Off. of the Vice President, Vice President Gore Announces New Steps Toward an Electronic Bill of Rights (July 31, 1998), https://govinfo.library.unt.edu/npr/library/news/electrc.html. While the FTC did pursue a "case-by-case enforcement strategy" on behalf of underaged internet users before Congress passed COPPA, its actions focused exclusively on demonstrably deceptive practices pursuant to its existing mandate for online interactions; agency leadership "felt [they were] unable to act in situations . . . where children's information was collected but no affirmative deception was present." HOOFNAGLE, *supra* note 6, at 159, 198.

47. CENTER FOR MEDIA EDUCATION, THE FIRST YEAR: A SURVEY OF SITES 5 (2001).

48. *See* 15 U.S.C. §§ 6501–6506. Under § 6501, "child" is defined as "an individual under the age of 13." *Id.* § 6501(1). Since fairly early on, the term "website" itself has been "broadly construed, and can include mobile and desktop applications; plug-ins on websites that capture data for metrics, social networking, or advertising purposes; advertising networks; location-based services; and services with voice over IP," with notable expansions coming with the renewed regulations published in 2013. HOOFNAGLE, *supra* note 6, at 200 (citing Consent Decree, United States v. W3 Innovations, LLC, No. CV11-03958 (N.D. Cal. Aug. 12, 2011) (FTC File No. 102 3251); Consent Decree, United States v. Bonzi Software, Inc., No. CV-04-1048 (C.D. Cal. Feb. 18, 2004); *see also* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (2013).

49. 15 U.S.C. § 6502(a)(1)–(2). While § 6502(a)(1) specifies that the website owners must have "actual knowledge" of child users in order to be liable for the statutory provisions, courts have endorsed a broad view of "actual knowledge" that enables regulators to consider this element fulfilled if the site can reasonably be believed to be appealing to underaged users. *See* HOOFNAGLE, *supra* note 6, at 200 (citing Consent Decree, United States v. UMG Recordings, Inc., No. CV-04-1050 (C.D. Cal. Feb. 18, 2004); Consent Decree, United States v. Jones O. Godwin, No. 11-CV-3846 (N.D. Ga. Feb. 1, 2012) (FTC File No. 1123033); Stipulated Order for Permanent Injunction and Civil Penalty Judgment, United States v. TinyCo., Inc., No. 14-CV-04164 (N.D. Cal. Sept. 16, 2014) (FTC File No. 132 3209)).

guidelines regarding the duration of data retention; parental rights to review collected information and withdraw consent for its further use; and clear and conspicuous privacy notices that provide information about any third parties that will collect, distribute, or receive data from users.[50]

Reactions to COPPA, and to the agency's enforcement of it (discussed in more detail below), have been mixed since its implementation. For instance, a year after COPPA's enactment, the CME began a survey of 153 commercial sites that targeted underaged users to ascertain the overall effect of the statute.[51] Within the surveyed sites, the CME found a significant increase in posted privacy policies, from around a quarter in 1998 to around three quarters at the time of the survey.[52] However, only a third of the sites included in the survey "had the link to the privacy policy in a 'clear and prominent' place on the home page," as required by the FTC.[53] Similarly, surveyed websites had a significant increase in attempts to obtain parental consent, but a majority failed to do so properly according to FTC guidelines.[54]

This report exemplifies the general reaction to COPPA and its immediate deployment: most parties involved expressed at least some degree of dissatisfaction. Consumer advocates, as discussed above, argued that the statute placed too much of a burden on (or too much faith in the ability of) parents to thoughtfully monitor their children's web activity in the face of the highly honed manipulation techniques employed by major advertisers.[55] Businesses, on the other hand, found its restrictions too tight, with several business leaders complaining that its provisions forced them to either frame every design and function choice around compliance or ban children from their services entirely.[56] And privacy watchdogs warned that COPPA and the FTC's published regulations based on it could create scenarios in which parents themselves were empowered to impinge on their children's reasonable

50. *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2013); *see also* HOOFNAGLE, *supra* note 6, at 202.

51. CENTER FOR MEDIA EDUCATION, *supra* note 47, at 6.

52. *Id.* at 8.

53. *Id.* at 10 (citing Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888, 59894 (Nov. 3, 1999)).

54. *Id.* at 12. To rectify these shortcomings, the center offered recommendations about communication between regulated entities and the agency. *Id.* at 16–17. In addition, the center's report encouraged the FTC to enlist the aid of the federal Department of Education in recruiting teachers to help educate students and parents about online safety issues. *Id.* at 16–18.

55. *See* HOOFNAGLE, *supra* note 6, at 212.

56. *Id.* at 210; *see also id.* at 215 (noting that banning children from web-based services simply encourages students to lie about their age rather than providing any substantive protection).

expectations of privacy while online, a concern that led Congress to rewrite COPPA to cover children aged thirteen and younger.[57]

B. FTC Enforcement of COPPA

The FTC followed a long-standing agency pattern as it began enforcement within this new statutory sphere. First, it sought to create room for the regulated businesses to define the best practices of the field, granting them some leeway for self-regulation.[58] These practices formed the basis for ensuing regulatory changes enacted by the agency, and in many cases were "tweaked into broader protections" than the industry players initially put forth.[59] Once these regulations were in place, the agency began to issue relatively mild warnings, followed by rapidly escalating penalties for repeat offenders or entities that engaged in practices that the agency has previously censured publicly.[60]

For example, in recent years, the agency has taken aim at key industry players and levied significant penalties. In 2019, the agency reached a settlement with Google and YouTube in which the companies paid a record-breaking $136 million to the agency and an additional $34 million to the State of New York.[61] The agency alleged that YouTube presented itself to advertisers as the "#1 website regularly visited by kids," while simultaneously claiming that it "did not have users younger than 13 on its platform and therefore channels on its platform did not need to comply with COPPA."[62] In addition to the monetary settlement, Google and YouTube agreed to build additional safeguards to identify content aimed at children, provide additional compliance training for employees, and affirm their commitment to providing notice to parents

57. *See id.* at 208–10 (citing Bryce Clayton Newell et al., *Privacy in the Family*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 104 (Beate Roessler & Dorota Mokrosinska eds., 2015); Benjamin Shmueli & Ayelet Blecher-Prigat, *Privacy for Children*, 42 COLUM. HUM. RTS. L. REV. 759 (2011)).

58. HOOFNAGLE, *supra* note 6, at 145–46.

59. *Id.* at 146.

60. *See id.* at 206. The FTC's COPPA penalties "averaged $30,000 in 2001" but escalated quickly, with a $400,000 settlement secured in 2004; this trend continued, and by 2011, the agency successfully levied a $3,000,000 penalty against Playdom. *See id.* (citations omitted) (showing several examples of escalating penalties for similar infractions).

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

62. *Id.*

and obtaining their consent.[63] The depth of that commitment, of course, remains to be seen.[64]

As required by the statutory text, the FTC has promulgated rules detailing a regulatory regime in order to effectuate COPPA's protections.[65] Most recently, the agency published a revised rule in 2013 that broadened the statutory term "operator" to include mobile applications and physical devices that interact with the internet.[66] The 2013 rule states that COPPA applies to

> operators of commercial websites and online services (including mobile apps . . .) directed to children under 13 that collect, use, or disclose personal information from children . . . . It also applies to operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13.[67]

This expansion into the so-called "Internet of Things" was a crucial step in ensuring that the constantly evolving library of online content available to underaged users, particularly content available only or primarily through applications on web-based devices such as mobile phones or "smart-home" hubs, remained firmly within the regulatory purview of the agency.[68]

---

63. *Id.*

64. While this settlement represents a significant step toward accountability, the FTC recently initiated additional action against numerous "major social media and video-streaming services," including YouTube. *See* Doss, *supra* note 30. The list of entities under investigation also includes Facebook, Twitter, Reddit, Discord, and others. *Id.* It is not yet known whether these investigations will uncover violations of COPPA on the part of YouTube or any of the other entities involved.

65. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.3 (2013).

66. *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (2013) (expanding the statutory terminology beyond static browser-accessed "websites" as such).

67. *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (July 2020), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions; *see also* Gianna Korpita, *It's a Small World After All: How Disney's Targeted Advertisements Implicate COPPA*, 19 J. HIGH TECH. L. 407, 415–17 (2019) (describing the FTC's adjustments to mobile device-based online activity, including cell phones and other "smart" devices).

68. *See* 16 C.F.R. § 312.3 (2013) (affirming the agency's mandate to protect children from unfair or deceptive practices including practices related to mobile games or networked devices). For a thorough discussion of the intersection of regulatory practice and the "internet of things," see generally Eldar Haber, *The Internet of Children: Protecting Children's Privacy in a Hyper-Connected World*, 2020 U. ILL. L. REV. 1209 (2020).

The agency's enforcement of COPPA has focused significantly on the parental notice facet of the statute.[69] Data collection and distribution are extremely important topics within the realm of digital privacy, but they are by their nature extremely difficult to monitor.[70] The agency has, instead, adopted a notice-and-consent regime as the basis for most of its enforcement efforts.[71] Overall, the agency's enforcement efforts surrounding such notice and consent practices have been admirable, and the FTC has developed considerable expertise in discussing, advocating for, and regulating digital privacy both for underaged users and the general population. However, given the advances in internet technology and computer science since the law's passage in 1998,[72] and the last substantive update to the agency's enforcement ruleset in 2013,[73] there is considerable room for improvement.[74]

Further, those concerned about digital privacy issues would be well-served to encourage the FTC to expand its perception of the COPPA mandate rather than expect new federal legislation, which—as will be discussed later—is just as likely to scale back protections as it is to buttress them.[75] Rather than encouraging the agency to recalibrate its entire COPPA posture to engage in the technical digging that would be needed to delve into the data collection and distribution itself, Part III of this Note suggests two ways for the agency to maintain its emphasis on notice and consent: first, with a new and more transparent regulatory

69. *See* Ariel Fox Johnson, *13 Going on 30: An Exploration of Expanding COPPA's Privacy Protections to Everyone*, 44 SETON HALL LEGIS. J. 419, 425 (2020) (citing Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501(9)) (characterizing COPPA as "designed to put parents in the driver's seat"); *accord* FED. TRADE COMM'N, POLICY STATEMENT OF THE FEDERAL TRADE COMMISSION ON EDUCATION TECHNOLOGY AND THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT 1 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Policy%20Statement%20of%20the%20Federal%20Trade%20Commission%20on%20Education%20Technology.pdf.

70. Debra A. Valentine, *Privacy on the Internet: The Evolving Legal Landscape*, FED. TRADE COMM'N (Feb. 11, 2000), https://www.ftc.gov/news-events/news/speeches/privacy-internet-evolving-legal-landscape.

71. *See* ANNE JOSEPHINE FLANAGAN ET AL., REDESIGNING DATA PRIVACY 9 (2020); HOOFNAGLE, *supra* note 6, at 202–04, 206; *see also* Damin Park, *Mining for Children's Data in Today's Digital World*, 38 J. NAT'L ASS'N ADMIN. L. JUDICIARY 320, 325–30 (2018) (discussing the various points of weakness in the FTC's current enforcement practices of COPPA, particularly regarding mobile device applications and behavioral marketing).

72. *See supra* Section I.A (discussing the development of the internet).

73. *See generally* 16 C.F.R. § 312 (2013).

74. For an example of newly minted privacy concerns springing from the last decade's technological growth, see, e.g., Jefferson Graham, *How Technology Made Us Bid Farewell to Privacy in the Last Decade*, USA TODAY (Dec. 23, 2019), https://www.usatoday.com/story/tech/2019/12/23/alexa-facebook-google-and-others-chipped-away-privacy-decade/2687455001/.

75. *See infra* Section III.B.2; *see also infra* note 126.

framework; and second, by engaging in a "bottom-up" campaign that will enlist parents as well as state officials in strengthening privacy protections for children.

III. PROPOSED POLICY CHANGES

With this history in mind, this Note suggests a two-pronged approach to strengthening the protections offered by COPPA. This approach includes complementary enforcement options that offer the agency (1) a set of comprehensible and easily applied tools for businesses to follow in managing their data policies and (2) a more robust and transparent civil penalty scheme applicable to entities that disregard the requirements.[76] To help this revamped enforcement regime make a significant difference in business practices surrounding the digital information of underaged users, this Part also includes options for the agency to act as an advocate by fostering greater awareness of digital privacy issues and sharing resources for parents and encouraging state and local authorities to have a more acute sense of ownership of these issues.

---

76. Recent developments in administrative law may prompt the FTC to pursue COPPA compliance with more force, simply due to a shift in available options for general enforcement. *See* M. Sean Royall et al., *A Watershed Moment? What Comes Next for the FTC in the Wake of AMG*, 35 ANTITRUST 103, 103, 105–07 (2021). As a rule, administrative agencies are limited by funding and personnel and must make decisions about enforcement based on practical considerations revolving around available resources weighed against potential impact. *See generally* Max Minzner, *Should Agencies Enforce?*, 99 MINN. L. REV. 2113 (2015). One relatively high-impact practice is "disgorgement," a method by which the FTC would "seek and obtain monetary relief in connection with requests for an injunction." Royall et al., *supra*, at 103; *see* Federal Trade Commission Act of 1914, 15 U.S.C. §§ 13(b), 53(b)(2). For a long time, the judiciary approved this practice. *See* FTC v. Com. Planet, Inc., 815 F.3d 593, 598 (9th Cir. 2016) (holding that restitution is feasibly within the terms of "any ancillary relief necessary to accomplish complete justice" (quoting FTC v. H. N. Singer, Inc., 668 F.2d 1107, 1113 (9th Cir. 1982))); FTC v. Ross, 743 F.3d 886, 890–92 (4th Cir. 2014); FTC v. Freecom Commc'ns, Inc., 401 F.3d 1192, 1202 n.6 (10th Cir. 2005); FTC v. Gem Merch. Corp., 87 F.3d 466, 468–70 (11th Cir. 1996); FTC v. Sec. Rare Coin & Bullion Corp., 931 F.2d 1312, 1314–15 (8th Cir. 1991). In *AMG Capital Management, LLC v. Federal Trade Commission*, however, the Supreme Court unanimously rejected this interpretation, holding that this portion of the FTC Act merely empowers the agency to stop "seemingly unfair practices from taking place while the Commission determines their lawfulness." AMG Cap. Mgmt., LLC v. Fed. Trade Comm'n, 141 S. Ct. 1341, 1348 (2021). Thanks to this judicial limitation on disgorgement, a significant portion of the FTC's enforcement bandwidth may now be available for a more heavily targeted enforcement of other active regulatory standards, including COPPA. *See* Royall et al., *supra*, at 106–07 (suggesting that the end of § 13(b) monetary damages may encourage the FTC to pursue "actions against companies violating . . . dozens of active rules promulgated by the FTC").

A. *Rethinking COPPA Enforcement at the FTC*

There are two broad layers of FTC action surrounding privacy concerns that could prove fruitful in terms of strengthening regulatory protections for underaged users. First, the agency should undertake complementary approaches within its own enforcement practices by providing streamlined, uniform standards for data notification for underaged users (with an eye toward a scalable system that could be adopted by regulated entities for all users, either as a commonly agreed-upon "best practice" or at the behest of a "super-regulatory" statute at the state level).[77] Second, the FTC should simultaneously reformulate its civil penalty practices to increase the prohibitive nature of the penalties it levies against entities that violate these regulations.[78]

1. Positive Federal Protection: Adjusting Expectations

A major issue with the current "patchwork" of legal obligations surrounding digital privacy is a lack of clarity regarding regulatory requirements.[79] Regulated entities must navigate an array of state-level statutes, narrow but weighty federal legislation, and incremental judgments by the FTC that have gradually defined the contours of what constitutes "unfair and deceptive" behavior vis-à-vis digital privacy.[80] And, unfortunately, previous attempts to generate a coherent set of best practices have largely been laughably permissive.[81]

---

77. *See infra* Section III.B.2.

78. While there are several possible models for such a reformulation, this Note will offer examples based on the EPA's penalty practices. *See infra* Section III.A.2.

79. *See* Lipman, *supra* note 16, at 787–88.

80. *See, e.g.*, Chander et al., *supra* note 4, at 1748–49; Doss, *supra* note 18, at 233–35. While the FTC is able to levy significant penalties for "unfair and deceptive" behavior, they are limited to cases in which regulated entities expressly misled the public. Lipman, *supra* note 16, at 790–93. The agency has noted in the past that their regulatory bandwidth is insufficient to address many of the issues in this field and has argued forcefully for stronger statutory protections for consumers against the practices of data brokers. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 5–7, 49–50 (2014).

81. Two examples, P3P and AdChoices, are particularly illuminating. P3P was an attempt to create a standardized and simplified version of privacy policies that could be automatically read and approved within browser settings, while the AdChoices campaign urged advertisers to include a clickable symbol within their advertisements that, when pursued, gave them "the choice to opt out of behavioral tracking." Lipman, *supra* note 16, at 796–98. Neither was successful. P3P failed because the technology for automating the process was too unsophisticated to actually prevent bad actors from bypassing users' preferences. *See id.* at 797. AdChoices was simply an unknown factor: users were not aware that it existed, and advertisers had little to no incentive to make it clear that customers had the power to opt out of their tracking. *See id.* at 798. The former accomplished nothing,

Recently, some scholars have suggested that the FTC could borrow the "nutrition label" concept from the Food and Drug Administration ("FDA") as a unified method for alerting users to the privacy practices of the online service providers they utilize.[82] Studies have shown that consumers respond readily to brief, easily digestible privacy notices; they take ownership of their data usage in ways that are uncommon with the more standard "wall of text" privacy policy notice practice.[83]

COPPA grants the FTC broad authority to define and regulate notice-and-choice regimes for parents, and the agency should make use of this power to promulgate a set of "label"-oriented standards that could be followed by online services that engage with underaged users.[84] The graphics for these "labels" could contain (or even consist of) a combination of QR codes[85] and active hyperlinks that lead to informative pages on the service provider's website that describe the rights and obligations of all parties involved, preferably with links to the FTC's online resources regarding COPPA. Additionally, service providers should be encouraged to expressly identify both the types of data retrieved and the ways in which these data will be utilized.[86]

---

and the latter was simply not used. *See id.* at 796–98; *see also* Park, *supra* note 71, at 346–48.

82. *See* Lipman, *supra* note 16, at 803–04; Park, *supra* note 71, at 350–51.

83. In one experiment, researchers found that "individuals changed their behavior based on the privacy notices" when they were able to "see how protective online sellers were of their privacy" specifically within the context of an "easy-to-comprehend privacy meter" that provided color-coded summaries of the site or service. Lipman, *supra* note 16, at 802.

84. *See* 15 U.S.C. § 6502(b).

85. QR (or "Quick Response") codes are specialized forms of "bar codes" that can be read by a variety of devices, including most modern cell phones, by scanning the code with a camera. The code then opens a web browser page directed at a URL specified within the QR code. For more on the history and use of this technology, see *Fukuda Yūichirō, The Little-Known Story of the Birth of the QR Code*, NIPPON.COM (Feb. 10, 2020), https://www.nippon.com/en/news/fnn20191214001/the-little-known-story-of-the-birth-of-the-qr-code.html; Yuhi Sugiyama, *From Japanese Auto Parts to Ubiquity: A Look at the History of QR Codes*, MAINICHI (Nov. 10, 2021), https://mainichi.jp/english/articles/20211109/p2a/00m/0bu/024000c. It should be noted, however, that there are privacy concerns baked into the technology behind QR codes; these concerns would need to be investigated and addressed prior to implementation as part of a new regulatory scheme. *See, e.g.*, Erin Woo, *QR Codes Are Here to Stay. So Is the Tracking They Allow*, N.Y. TIMES (July 26, 2021), https://www.nytimes.com/2021/07/26/technology/qr-codes-tracking.html; Tatum Hunter, *QR Codes Are a Privacy Problem — But Not for the Reasons You've Heard*, WASH. POST (Oct. 7, 2021, 7:00 AM), https://www.washingtonpost.com/technology/2021/10/07/are-qr-codes-safe/.

86. *See* Lipman, *supra* note 16, at 802–04. The standard example given is to offer users "a grid with the label 'information we collect' on the vertical axis and 'ways we use your information' on the horizontal axis." Park, *supra* note 71, at 350. Most recommend making

Initially, it makes the most sense to implement such a "nutrition label" scheme strictly under the auspices of a statute such as COPPA in order to obviate the need for a broader general statute. Once in place, however, this program has the benefit of being easily scalable and adjustable for the needs of different statutes or user groups as the law surrounding privacy shifts. For instance, specific label variants could be put forth that would indicate that a website or service is robust enough to offer full protections for health data under HIPAA or financial information under the Fair Credit Reporting Act ("FCRA").[87] This practice would enable service operators to demonstrate that they have taken the appropriate steps to meet their statutory obligations while simultaneously giving users both peace of mind regarding the uses to which their data are being put as well as resources to restrict or remove permissions as allowed by law.

The primary risk associated with implementing a "privacy nutrition label" scheme as part of COPPA enforcement is, of course, the likelihood of lawsuits accusing the agency of overreaching their statutory mandate. As mentioned, the agency's authority under COPPA is quite broad, and new regulations that simply codify new ways for regulated entities to be in compliance are likely to be analyzed with deference by federal courts.[88] Perhaps the easiest way to ensure that litigation does not overly hinder such a plan would be to make the "data nutrition label" scheme an opt-in endeavor rather than a strict requirement: the agency could, in its rulemaking capacity, make it clear that online service providers catering to children are not obligated to make use of this scheme, but that if they do choose to do so, the simple act of putting together the label and its attendant information would serve to ensure compliance with COPPA and thus give the regulated entity a clearly marked path to avoid enforcement actions.[89] With care and attention to detail, a notice-and-

---

these grids machine-readable for ease of use, which further supports the idea of using QR code technology. *See, e.g.*, *id.* at 350–51.

87. *See, e.g.*, 45 C.F.R. § 164 (2013) (detailing the standards of the "HIPAA privacy rule"); Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681(a)(4) (establishing a duty on consumer reporting agencies to "exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy"); *see also* Lipman, *supra* note 16, at 787–88.

88. The judiciary is likely to analyze this question under the so-called "Chevron Doctrine," which prevents courts from substituting their own judgment for that of a federal agency as long as the agency's action is reasonable and does not expressly violate the statutory language. *See* Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837, 865 (1984); *but see* West Virginia v. EPA, 142 S. Ct. 2587 (2022) (using the "Major Questions Doctrine" to constrain EPA regulatory authority).

89. Savvy service providers would know that, while alterations to compliance procedures may impose up-front costs, the additional clarity provided by such a procedure

choice regime that borrows from the nutrition label convention used by the FDA could provide a much more transparent system through which parents can monitor their children's online activity and protect their privacy.

2. Negative Federal Protection: Recalibrating the Penalties

Under the authority granted by COPPA, the FTC has the authority to levy civil penalties against entities that violate agency regulations regarding the digital privacy of underaged internet users.[90] The agency's enforcement efforts thus far have been relatively organic, flowing out of established "best practices" into a series of escalating warnings and finally into substantial penalties for repeat or egregious offenders.[91] This system has the regulatory advantage of imposing "tremendous public relations cost[s]" for violators, as businesses that are penalized are frequently given "'front-page' treatment in the *Wall Street Journal*" and other media outlets.[92] However, in many cases, even large penalties or settlements are fairly minor within the broader sweep of the regulated institutions' balance sheets.[93] Furthermore, without clearly published penalty rubrics, regulated entities must keep up with an ever-expanding portfolio of consent decrees and settlement documents, where available, rather than reference consolidated information regarding agency priorities and penalty procedures.

If the FTC's goal is to actively discourage violations of COPPA while providing a more visible and clearly defined procedure for penalty assessment, its leadership could look to one of its sister agencies, the Environmental Protection Agency. When assessing penalties against polluters, the EPA generates a "preliminary deterrence figure" based on two primary components: a benefit component and a "gravity" component.[94] The first is intended to represent the economic benefit that

---

would almost certainly reduce costs in the long term. *See* Chander et al., *supra* note 26, at 660.

90. 15 U.S.C. § 6502(c) (alteration in original) (ordering the agency to consider violations of COPPA regulations as de facto "unfair or deceptive act[s] or practice[s]" as described in 15 U.S.C. § 57a(a)(1)(B), which gives the agency authority to bring litigation to compel payment of civil penalties as authorized by 15 U.S.C. § 45(m)).

91. *See supra* Section II.B; *see also supra* note 60.

92. HOOFNAGLE, *supra* note 6, at 166.

93. *See* Press Release, Fed. Trade Comm'n, *supra* note 61. While this penalty of $190 million is certainly not small, it amounts to less than one percent of Alphabet's revenue for the year ($161.9 billion). *See* Tiago Bianchi, *Annual Net Income Generated by Alphabet from 2011 to 2022*, STATISTA (Feb. 13, 2023), https://www.statista.com/statistics/513049/alphabet-annual-global-income/.

94. ENV'T PROT. AGENCY, POLICY ON CIVIL PENALTIES 3–5 (1984) [hereinafter EPA POLICY]; *see also* ENV'T PROT. AGENCY, A FRAMEWORK FOR STATUTE-SPECIFIC APPROACHES

the violator gained by shirking its ecological responsibilities, thereby offsetting the perceived benefit of the pollution.[95] The agency's policy directives list numerous potential benefits including delayed costs, avoided costs, and competitive advantage.[96] In each assessment, the agency weighs these categories to assign an economic value to the violation; this value becomes the cornerstone of the deterrence figure and is rarely decreased except in instances wherein the benefit amount would be "insignificant" or under fairly extreme situations in which proceeding to trial would be against "compelling public concerns."[97]

Part of the goal of the EPA's rubric is to ensure that violators are left in a worse position than they would have by complying with the law in the first place, which compels the agency to move beyond the "benefit component."[98] Thus, the "gravity component" is a crucial second piece of the penalty assessment puzzle. When weighing the gravity of an offense, agency representatives must consider several factors. The actual or possible harm itself, based on such subfactors as the nature and amount of the pollutants in question, the "sensitivity of the environment," and the duration of the polluting activity are all crucial components of any offense.[99] In addition, EPA staff must also consider the relative importance of the violated rule within the context of the entire regulatory framework:

> For example, if labelling is the only method used to prevent dangerous exposure to a chemical, then failure to label should result in a relatively high penalty. By contrast, a warning sign

---

TO PENALTY ASSESSMENTS: IMPLEMENTING EPA'S POLICY ON CIVIL PENALTIES 2–3 (1984) [hereinafter EPA FRAMEWORK]. For a thorough discussion of the EPA's enforcement posture since its inception under President Nixon, see generally JOEL A. MINTZ, ENFORCEMENT AT THE EPA: HIGH STAKES AND HARD CHOICES (rev. ed. 2012).

95. *See* Civil Monetary Penalty Inflation Adjustment, 87 Fed. Reg. 1676, 1676 (Jan. 12, 2022) (to be codified at 40 C.F.R. pt. 19) ("The EPA's civil penalty policies . . . take into account a number of fact-specific considerations, *e.g.*, . . . any economic benefit gained by the violator as a result of its noncompliance . . . .").

96. *See* EPA FRAMEWORK, *supra* note 94, app. at 6–11.

97. *Id.* app. at 11–13. Such "compelling public concerns" include cases in which agency officials deem it likely that the judiciary will create an adverse precedent if litigation proceeds, instances wherein a quick settlement is necessary to "avoid or terminate an imminent risk to human health or the environment," and cases where "extreme financial burden[s]," such as plant closures or bankruptcy, might accrue to the communities involved. *Id.* app. at 12. This last possibility comes with a cautionary note, warning that "the Agency will give the perception that shirking one's environmental responsibilities is a way to keep a failing enterprise afloat" if this option is used too frequently. *Id.* app. at 13.

98. EPA POLICY, *supra* note 94, at 3 ("Both deterrence and fundamental fairness require that the penalty include an additional amount to ensure that the violator is economically worse off than if it had obeyed the law.").

99. EPA FRAMEWORK, *supra* note 94, app. at 14–15.

> that was visibly posted but was smaller than the required size would not normally be considered as serious.[100]

Lastly, agency assessors must consider the size of the violator, with an eye toward ensuring that the penalty is large enough to be a meaningful deterrent to future bad actions for any given polluter.[101]

With these two components in hand, the EPA official has reached the "preliminary deterrence figure," which then serves as a starting point for negotiations with the offending party.[102] At this point, the agency begins to consider—and negotiate—factors that could reduce the penalty, often with the goal of encouraging the violator to take immediate action to mitigate the pollution.[103] These factors include the degree of culpability and subsequent cooperation with agency investigators, as well as the violator's history (or lack thereof) of previous offenses.[104] Lastly, the violator's ability to actually pay the penalty is weighed in the balance;[105] for instance, in a case involving emissions control mechanisms in motor vehicles, the EPA noted that Advanced Flow Engineering, Inc. would only pay a total penalty of $250,000 since "the company has a limited financial ability to pay a higher penalty."[106]

It is worth noting again that the FTC has not published any rubric for assessing penalties for privacy infractions under COPPA, largely due to internal consensus that the time and effort required to do so would not be worthwhile.[107] The lack of publicly available penalty rubrics also gives the agency a certain degree of flexibility in enforcement tactics.[108] However, setting out more formal guidelines on privacy enforcement

---

100. EPA POLICY, *supra* note 94, app. at 14.

101. EPA FRAMEWORK, *supra* note 94, app. at 15.

102. *See* EPA POLICY, *supra* note 94, at 4–5.

103. *See id.* at 5–6 ("[S]wift correction of identified environmental problems must be an important goal of any enforcement action. In addition, swift compliance conserves Agency personnel and resources.").

104. *See* EPA FRAMEWORK, *supra* note 94, app. at 16–22.

105. *See id.* app. at 23 ("The Agency will generally not request penalties that are clearly beyond the means of the violator . . . . At the same time, it is important that the regulated community not see the violation of environmental requirements as a way of aiding a financially troubled business.").

106. *Advanced Flow Engineering, Inc., Clean Air Act Settlement*, ENV'T PROT. AGENCY, https://www.epa.gov/enforcement/advanced-flow-engineering-inc-clean-air-act-settlement#penalty (July 25, 2022); *see also* Press Release, Env't Prot. Agency, Justice Department and EPA Reach Clean Air Act Settlement with Advanced Flow Engineering for Selling Defeat Devices (July 27, 2021), https://www.epa.gov/newsreleases/justice-department-and-epa-reach-clean-air-act-settlement-advanced-flow-engineering ("The . . . penalty . . . was based on [the company's] financial situation.").

107. *See* HOOFNAGLE, *supra* note 6, at 82–83, 118.

108. *See id.* at 118 (explaining how the agency's policy-making enforcement agenda is flexible and fluid).

would allow the agency to reference concrete, objective rules that prioritize penalties sized to meet the fiscal landscape of regulated entities. This approach, in conjunction with the "nutrition label" positive enforcement scheme discussed previously,[109] would create a much stronger incentive for regulated businesses to color within the regulatory lines.

If the FTC decided to implement a regime similar to the EPA's benefit and gravity scheme, they could do so handily. For instance, in the previously cited example of Google and YouTube,[110] the FTC would need to determine the economic benefit derived by the violations in question.[111] They would then need to establish and apply a rubric to determine the severity of the violation, making inquiries about the number of underaged users whose privacy was jeopardized by the violator's actions; the length of time such actions were ongoing and whether or not the violator has committed similar offenses in the past; and the depth and breadth of the "spread" of this data.

This information could then be triangulated into a "gravity" penalty component similar to that generated by the EPA's enforcement guidelines, providing a "preliminary deterrence figure" that could then be the starting point for settlement negotiations with the offender.[112] Within these negotiations, the agency could press the violators to not only cease the existing behavior but also take steps to curtail the further use of the retrieved data as steps to mitigate their liability. A public penalty rubric would thus provide a concrete mechanism for making noncompliance too costly for potential violators to risk exposure while simultaneously providing an incentive for violators to consider possible mitigative action after the fact in order to reduce the eventual penalty amount.

B. Leveraging Privacy from the Ground Up

In addition to striking a more robust and comprehensive enforcement stance, the agency should adopt a more proactive approach to informing parents of their rights under COPPA and provide them with a more conspicuous and easy-to-use avenue to report suspected breaches of the

109. *See supra* Section III.A.1.

110. *See* Press Release, Fed. Trade Comm'n, *supra* note 61.

111. Unlike cases before the EPA, of course, matters of privacy violation would not focus on avoided or delayed costs, or even specifically on competitive advantage. *See* EPA POLICY, *supra* note 94, app. at 6–11. Rather, the "benefit" component will most likely need to be directly tied to the value gained by repackaging and selling the data in question or using it for internal advertising. *See id.* app. at 6, 9–10.

112. *See id.* app. at 6, 13–16.

statute to agency personnel. In a similar "advisory" vein, the agency could build on its success advising the California legislature in the passage of the California Consumer Privacy Act and help create multiple state-level "super-regulators" that lessen the pressure on the FTC as a sole actor.

1. Encouraging Parental Involvement

Concerned parents often turn to the legal system to protect their children from suspected violations of privacy, but their efforts are typically frustrated by the lack of an explicit private right under COPPA.[113] This challenge is compounded by a relative dearth of actionable guidance from the FTC. The FTC's website, for instance, has a well-crafted page detailing the rights of children under COPPA.[114] However, the only offered method of redress is the general fraud report website.[115] While this route gives parents some degree of input, the main page itself can and should include a more thorough discussion of what

113. While COPPA does not enumerate a private right of action, concerned parents have repeatedly attempted—with little success—to bring suit under its auspices. For instance, in August of 2017, a concerned parent filed lawsuits against both Viacom and Disney claiming that many of their gaming apps, including those related to child-oriented intellectual properties including Toy Story, DuckTales, and Star Wars, violate children's right to privacy under COPPA. *See* Complaint at 10–12, Rushing v. The Walt Disney Co., No. 17-cv-4419 (N.D. Cal. Aug. 3, 2017). The suit against Viacom survived a motion for summary judgment claiming that the parent had no standing under COPPA, suggesting that there might be room for a somewhat broad view of the statute's parameters. *See* Rushing v. Viacom Inc., No. 17-cv-04492, 2018 WL 4998139, at *1 (N.D. Cal. Oct. 15, 2018).

However, the recent judicial trend has been to disclaim any private right of action under federal law. In *Manigault-Johnson v. Google, LLC*, concerned parents attempted to bring a class action suit against YouTube, Google, and their parent company, Alphabet, for privacy violations committed against underaged internet users. *See* Manigault-Johnson v. Google, LLC, No. 18-cv-1032, 2019 WL 3006646, at *2 (D.S.C. Mar. 31, 2019). The court acknowledged that private action under state law is not preempted by COPPA. *See generally id.* at *10 (citing *In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 293 (3d Cir. 2016)). Even so, the judge dismissed the lawsuit, finding both that the plaintiffs had failed to demonstrate deceptive practices that could properly be considered "harm" under state law and that the plaintiffs appeared to be using "the vehicle of state law to privately enforce the provisions of COPPA, which Congress clearly intended to preclude." *Id.* at *6, *18–20.

A district court in California recently reached a similar conclusion in a lawsuit involving Google, and—upon appeal—the case was remanded, but only to determine whether a state law claim could survive without reference to COPPA. *See generally* Hubbard v. Google LLC, No. 19-cv-07016, 2021 WL 2711748 (N.D. Cal. July 1, 2021), *rev'd sub nom.* Jones v. Google LLC, 56 F.4th 735 (9th Cir. 2022). It is thus fair to say that, at present, parents are left with little hope for successful private action under federal law.

114. FED. TRADE COMM'N, NET CETERA: CHATTING WITH KIDS ABOUT BEING ONLINE 23–25 (2014), https://consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0001-netcetera_0.pdf.

115. *Report to Help Fight Fraud!*, FED. TRADE COMM'N, https://reportfraud.ftc.gov/#/ (last visited Mar. 13, 2023).

parents can expect vis-à-vis protection of their children's information and online privacy in general.

At minimum, the FTC should make it much clearer that private lawsuits are unlikely to succeed due to the lack of a specified private right within the statutory language of COPPA. Instead, the agency should urge parents to both report bad actors to agency staff via the available online forms and contact state authorities who have standing to file claims on their behalf if warranted. This response could lead to collaboration between parents, state law enforcement officials, and the agency itself that may prove singularly potent.

In tandem with this effort to educate and equip parents to more effectively advocate for their children, the agency would be well-served to enlist the aid of state-level departments of education in helping raise awareness of privacy risks for children. This approach could provide a much-needed boost to parental involvement in seeking stricter privacy protections for their children at the state level, which would only help the agency's goal of promoting a healthy digital environment for underaged users. And increased parental involvement could then be parlayed into more robust state-level statutes, discussed in more detail below.

2. Encouraging the Growth of "Super-Regulators"

In addition to having the right to pursue COPPA claims directly, state governments have the right to pass laws requiring more stringent privacy practices than federal statutes.[116] By encouraging states to ratchet up their privacy requirements for underaged users, the agency could potentially create a network of state-level "super-regulators," described in brief below, that raises the bar for privacy regulation without needing federal legislation.

A "super-regulator" is a government entity that for one reason or another sets regulatory standards for entire swaths of industry.[117] The most basic type of super-regulator is often described as a "Delaware" regulator: given the years of expertise gained by the Delaware judiciary in parsing corporate law, corporations self-select Delaware as the preferred jurisdiction not only for incorporation but also for examining legal questions of corporate structure.[118] By contrast, a "Brussels"-style

116. *U.S. State Privacy Laws*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/privacy-laws/state-laws/ (last visited Mar. 13, 2023).

117. *See generally* Chander et al., *supra* note 4.

118. *Id.* at 1740–41. Chander and company eschew the traditional view of this phenomenon, which asserts that Delaware's body of corporate law represents a regulatory "race to the bottom" in which the state attempted "corner[] the market for incorporations through dubious efforts to favor corporate officers and directors." *Id.* at 1739–41. Instead,

regulatory scheme imposes high standards that force industries to choose between adopting full compliance across all products, wherever they end up being distributed, or paying to create and monitor multiple types of production facilities, often at greater cost than simply complying with the higher standards across the board.[119] Milder regulatory schemes provided by other jurisdictions are effectively overridden, as the regulated entities can simply ignore the lower thresholds entirely and focus on compliance with the more demanding regime.[120]

Striking a balance between the two is the so-called "California"-style super-regulator. Similar to the Brussels iteration, this type of super-regulator provides a more stringent set of guidelines for a given industry than the current baseline.[121] Unlike its European counterpart, however, this classification of super-regulator provides impetus not to the regulated industry but to other similarly situated jurisdictions: by providing examples of what is possible, a "California"-style super-regulator can inspire other jurisdictions within its ambit to craft similar schemes.[122] The effects of these categories of super-regulators can differ in small but important ways that provide both shape and velocity to the ongoing regulatory conversation.[123] And it is this type of super-regulator that the FTC could encourage by embracing a more proactive advisory

---

the authors endorse the view that by empowering its judiciary to develop expertise in corporate law to a degree that made them the de facto experts, Delaware's legislature provided businesses with an overwhelmingly attractive option for incorporation. *Id.* at 1741 (first citing Ralph K. Winter, Jr., *State Law, Shareholder Protection, and the Theory of the Corporation*, 6 J. LEGAL STUD. 251, 254 (1977); and then citing ROBERTA ROMANO, THE GENIUS OF AMERICAN CORPORATE LAW 37–39 (1993)).

119. *Id.* at 1744–45.

120. Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 8 (2012). Bradford outlines three requirements for what he labels the "Brussels Effect": first, there must exist a unilateral regulator of a compelling market; second, that regulator must have the legal heft to create strict rules for "inelastic targets" thus ensuring that the rules are difficult to evade; and third, the regulated entity must operate in an indivisible fashion that would be impractical to split along a variety of regulatory fault lines. *See id.* at 10–12.

121. Chander et al., *supra* note 4, at 1743–44.

122. *Id.* at 1742–43. The first and most well-known instance of the "California effect" is within the context of environmental regulation: California's automobile emissions standards were grandfathered into the amended Clean Air Act of 1966 (CAA). Ann E. Carlson, *Iterative Federalism and Climate Change*, 103 NW. U. L. REV. 1097, 1111 (2009). Shortly thereafter, the 1970 version of the CAA "explicitly recognized California as a superregulator," granting it the sole authority to "set stricter-than-federal standards" with the proviso that "other states could then opt to follow California's standards," an opportunity seized by twelve states and the District of Columbia. Chander et al., *supra* note 4, at 1743–44.

123. *See, e.g.*, Chander et al., *supra* note 4, at 1743; *see also* Carlson, *supra* note 122, at 1097–99 (crediting the federal government with shaping and enabling state responses to climate change through a dynamic process of "iterative federalism").

role for state legislatures eager to respond to the aforementioned parental concern vis-à-vis children's digital privacy.

In 2018, two legislative bodies separately enacted privacy statutes that have successfully reframed the conversation surrounding online information, acting as "California-style" super-regulators for the field of digital privacy: the European Parliament and Council of the European Union enacted the General Data Protection Regulation ("GDPR") in April 2016, and the California state legislature enacted the CCPA.[124] There are significant substantive differences between the GDPR and the CCPA,[125] but they share a common effect: legislative entities across the globe have proposed, argued, and, in some cases, enacted their own versions of each.[126] And, crucially, the latter was enacted with significant input and

---

124. Chander et al., *supra* note 4, at 1734; *see also* Brittany A. Martin, *The Unregulated Underground Market for Your Data: Providing Adequate Protections for Consumer Privacy in the Modern Era*, 105 IOWA L. REV. 865, 880–83 (2020) (describing the overall contours of the CCPA as well as the legislative history of its passage).

125. The statutes also, of course, share significant similarities: for instance, both create protections that follow data from consumer, to procurer, to broker, and to end-use purchaser; both establish the capacity of any piece of data to positively identify the original user to be the primary consideration for protective status; both mandate rights of notice and access for consumers; and both confer a private right of action. *See* Chander et al., *supra* note 4, at 1749–53, 1759; *Does the CCPA Have a Private Right of Action?*, TRUEVAULT, https://www.truevault.com/learn/ccpa/does-the-ccpa-have-a-private-right-of-action (last visited Apr. 27, 2023).

However, there are core philosophical differences between the two that render them distinct in posture. The GDPR regards privacy as a core human right that can be, in essence, "rented" but never fully divested, and states broad, general principles to be fleshed out by both government institutions and regulated entities. *See* Chander et al., *supra* note 4, at 1755–58. By contrast, the CCPA treats privacy as a commodity that can be exchanged on a semi-permanent basis, the regulation of which boils down to discrete, granular requirements that lay predictable and obvious burdens on service providers that fall under its umbrella. *See id.* at 1755–60. The GDPR places a heavy burden on businesses that use and process data, requiring active consent from consumers at each new transaction including the use of their data, while the CCPA simply places a burden on businesses to provide notice if they plan to make use of such data. *See id.* at 1756–57; General Data Protection Regulation 2016/679, arts. 6(1)(a)–(f), 83(5), 2016 O.J. (L 119) 1; CAL. CIV. CODE § 1798.100(b) (West 2023). And where the GDPR "consists of broad standards in its text" and, through its sweeping encouragement of collaboration, "exemplifies collaborative governance," the CCPA "establishes limited but granular requirements that California's attorney general has fleshed out further in recently promulgated regulations." *See* Chander et al., *supra* note 4, at 1760.

A final, if less substantive, distinction is in the relative density of the statutes: the GDPR is, in essence, a full "title," with multiple chapters dividing its more than 100 pages. *See id.* at 1746. The CCPA is closer to twenty-five pages. *Id.* As Chander, Kaminski, and McGeveran put it, "[i]f the GDPR is a doctoral thesis, the CCPA is a term paper written the night before the deadline." *Id.*

126. Chander et al., *supra* note 4, at 1734–37. This response provides an interesting situation in which Brussels and California are simultaneously acting as both Brussels- and California-style super-regulators. On the one hand, most digital stakeholders are loathe to

support from FTC personnel, providing a potential roadmap for future development of state statutes to continue to evolve privacy law at the state level in the United States.[127]

The broad reach of these laws does, to a degree, beg an obvious question: "if indeed European or Californian regulation will be applied globally de facto, why then should anyone else legislate?"[128] Given the rapid advancements in technology, legislatures will likely need to revisit this issue on a regular basis in order to effectively address new vistas of digital privacy that could not have been covered by previous legislation. American federalism thus provides a more fruitful avenue for the energy of concerned parents or teachers than private litigation: state-level legislators are apt to be more responsive to the demands of their constituents than federal judges have been to private citizens attempting to co-opt enforcement of COPPA through the courts.

And as these states consider new legislative action, they have the option to avail themselves of the expertise of the FTC. This type of state-

---

attempt to parse out differences in users' legal status, as it is more efficient to simply comply with the more stringent regulation—a "Brussels" effect in action. *See id.* at 1744–45. Simultaneously, however, lawmaking bodies at both the national and subnational levels have taken a buffet-style approach to the GDPR and CCPA in enacting their own statutes, generating a complementary "California" effect. *Id.* at 1745–47.

Both effects are worth pointing out. However, the "California" effect is more important for the purposes of this Note, as it provides a context within which the FTC can shape developing law. This trend is particularly evident when looking at state-level laws in the United States. *See id.* at 1772–76. Connecticut, Massachusetts, and North Dakota have all extensively drawn from the CCPA to create new privacy statutes. *See id.* Multiple other states have at least considered doing so in the last few years. *See id.* at 1775–76. And the Uniform Law Commission ("ULC"), responsible for model statutes such as the Uniform Commercial Code, Uniform Probate Code, and Model Penal Code, is developing a "comprehensive legal framework for the treatment of data privacy" that relies on the CCPA, at least in part. *See* Katie Robinson, *New Drafting and Study Committees to Be Appointed*, UNIF. L. COMM'N (July 24, 2019, 4:37 PM), https://www.uniformlaws.org/committees/community-home/digestviewer/viewthread?MessageKey=bc3e157b-399e-4490-9c5c-608ec5caabcc&CommunityKey=d4b8f588-4c2f-4db1-90e9-48b1184ca39a&tab=digestviewer#bmbc3e157b-399e-4490-9c5c-608ec5caabcc.

While some federal legislators have proposed digital privacy statutes, they tend to draw on older legislation, and in fact may represent "a backlash against the CCPA," with a focus on preempting more protective state laws by offering scaled back regulation at the federal level. Chander et al., *supra* note 4, at 1779–80; *see also* Darius Tahir, *Pelosi Puts Privacy Marker Down*, POLITICO (Apr. 15, 2019, 10:00 AM), https://www.politico.com/newsletters/morning-ehealth/2019/04/15/pelosi-puts-privacy-marker-down-424986 (quoting former House Speaker Nancy Pelosi as saying "the Republicans would want preemption of state law. Well, that's just not going to happen . . . . We in California are not going to say, 'You pass a law that weakens what we did in California.'").

127. *See* Chander et al., *supra* note 4, at 1782.

128. *Id.* at 1738.

level action has enormous potential for reshaping the legal landscape surrounding privacy law. By leveraging its collective expertise with the technologies involved, the FTC can serve as a "federal lobbyist" of sorts at the state level, shaping state-level legislation to create more robust protections for consumers of all ages.

As an example, the FTC could actively promote Vermont's unique privacy statute to other state legislatures. In May of 2018, the Vermont state legislature passed a privacy statute that focused on data brokers, business entities that package and sell information after its collection, rather than on data harvesters, and the entities that actively collect data from websites, apps, and smart devices.[129] This statute requires data brokers to register annually with the Vermont Secretary of State and provide information about their "data collection practices, databases, sales activities, and opt-out policies that are applicable to the brokered personal information of minors."[130] Likewise, it imposes a strict set of guidelines for broker security standards, placing the burden on these entities to protect the integrity of consumer information or face stiff penalties.[131] Other states have lagged behind Vermont in applying regulatory pressure to this side of the data and advertising business. The FTC could help resolve this situation by educating state officials on the relative merits and benefits of Vermont's brokerage regulations—and, in particular, by encouraging states to consider a stricter version of Vermont's statute applicable to data generated from underaged users. While Vermont's population is likely not large enough to qualify its regime as "super-regulatory" in nature, the FTC could take this statute as a template and present it to other state legislatures looking to pass similar laws.[132]

By helping different states craft legislation that properly regulates industry actors, the FTC can generate a cascade of improved protections that may encourage data brokers to assume higher standards as a general practice.

---

129. *See* VT. STAT. ANN. tit. 9, § 2446 (2019); *see also* Martin, *supra* note 124, at 883–84.

130. *See* tit. 9, § 2446(a)(3)(F).

131. tit. 9, § 2446(b).

132. The agency could take a similar tactic with the recently passed California Age-Appropriate Design Code Act, which goes so far as to impose a legal obligation on regulated businesses to "consider the best interests of children when designing, developing, and providing that online service, product, or feature," and to prioritize said interests over their own commercial interests in case of any conflict. California Age-Appropriate Design Code Act, Assemb. B. 2273, 2022 Leg., Reg. Sess. § 1798.99.29(a)–(b) (Cal. 2022). As this statute does not take effect until 2024, its impact on the regulatory landscape is still to be determined. For further reading, see Natasha Singer, *Sweeping Children's Online Safety Bill is Passed in California*, N.Y. TIMES (Aug. 30, 2022), https://www.nytimes.com/2022/08/30/business/california-children-online-safety.html.

CONCLUSION

A recent surge in consumer concern about data privacy has generated considerable impetus for regulation of technology companies, but there is no indication that Congress is close to creating substantive privacy law. In the absence of new federal legislation, other actors must explore options to ensure that the law does not fall irretrievably behind the technology. Empowered by COPPA, the FTC is poised to do exactly that, both by catalyzing state and local action and by recalibrating its own regulatory framework. By enacting the suggestions in this Note, the FTC can continue to develop a more robust privacy regime in order to protect underaged users.