Harvard Journal of Law & Technology
Volume 37, Number 3 Symposium 2023

INFORMING FUTURE PRIVACY ENFORCEMENT BY EXAMINING 20+ YEARS OF COPPA

Serge Egelman[*]

ABSTRACT

While the United States currently has no comprehensive privacy law, the Children's Online Privacy Protection Act ("COPPA") has been in effect for over twenty years. As a result, the study of compliance issues among child-directed online services can yield important lessons for future enforcement efforts and can be used to inform the design of future state and federal privacy laws designed to protect people of all ages. This Essay describes relevant research conducted to understand privacy compliance issues and how that has led the author to several recommendations for how privacy enforcement can be improved more generally. While these recommendations are informed by the study of child-directed services' compliance with COPPA, they are applicable to future state and federal privacy laws aimed at protecting the general public (i.e., not just children).

Despite evidence of thousands of COPPA violations (e.g., one study found evidence that a majority of child-directed mobile apps appeared to be violating COPPA in various ways), the Federal Trade Commission ("FTC") and state attorneys general — the only entities with enforcement authority under the law — pursue few enforcement efforts each year. Despite having competent personnel, these organizations are heavily constrained and under-resourced — as a result, enforcement by regulators is simply not seen as a credible threat by software developers. Research has found that developers are much more concerned with apps being removed from app stores (i.e., due to enforcement of platforms' terms of service) than with the largely theoretical threat of regulatory enforcement. Yet the burden of COPPA compliance largely rests on numerous individual app developers. Thus, shifting enforcement efforts to the far-fewer platforms that distribute the apps (and make representations about their privacy and security

[*] Research Director, International Computer Science Institute (ICSI); Department of Electrical Engineering and Computer Sciences, University of California, Berkeley. The author wishes to thank Susan Landau and Nathan Reitinger for feedback on early drafts of this Essay; Mihailis Diamantis and Rishab Nithyanand for organizing the *Harvard JOLT*-UIowa IBL Symposium: Beyond the FTC, which was the forcing function for putting these thoughts to paper; as well as the other participants of that workshop. The author's own research described in this Essay was supported by the U.S. National Science Foundation, National Security Agency, Department of Homeland Security, and the Center of Long-Term Cybersecurity at U.C. Berkeley.

properties) and data recipients (who ultimately receive consumers' identifiable data) would likely yield better outcomes for consumers, while allowing the FTC to better focus its enforcement efforts and have greater impact.

Based on these observations, this Essay proposes a new enforcement framework. In this framework, compliance burdens are shifted away from the numerous individual online services to the fewer bigger players who are best positioned to comply: platforms and third-party data recipients. The FTC's limited resources can then focus on those entities at the top of the data food chain. Enforcement targeting the other, more numerous, individual online services could be left to a novel mechanism that uses a private right of action to foster more robust industry self-regulation through FTC-approved certification programs.

TABLE OF CONTENTS

I. INTRODUCTION

The Children's Online Privacy Protection Act ("COPPA")[1] was first enacted in 1999. While periodic rulemaking has added various refinements, its main provisions have now been the law of the land for over twenty years. While only applying to data collected from U.S. individuals under the age of thirteen, it is a relatively comprehensive privacy law. Unlike sectoral laws (e.g., the Health Insurance Portability and Accountability Act ("HIPAA"),[2] the Family Educational Rights and Privacy Act,[3] or the Gramm-Leach-Bliley Act ("GLBA")),[4] it governs how data should be collected from children, regardless of the type of service that they are using. COPPA applies to online services that are either specifically directed to children under the age of thirteen or online services that have "actual knowledge" that they are collecting

[1] 15 U.S.C. § 6501 *et seq.*

[2] Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of the U.S. Code).

[3] 20 U.S.C. § 1232g; 34 C.F.R. § 99.3 (2021).

[4] 15 U.S.C. § 6801 *et seq.*

data from children under the age of thirteen.[5] It requires that these services post privacy policies that describe their practices and forbids services from collecting certain types of personal information from children without parental consent.[6]

Despite being in effect for over twenty years, and despite those creating child-directed content being largely aware of its existence (e.g., a recent study of mobile app developers found that eighty percent of developers surveyed claimed familiarity with COPPA),[7] compliance rates with COPPA remain woefully inadequate. For example, research has found that a majority of child-directed Android apps appeared to be violating COPPA.[8] In follow-up research aimed at understanding the reasons for these high rates of potential noncompliance, researchers found that this was largely due to developers' misunderstandings of their obligations, as well as a misplaced belief that others were performing compliance checks on app developers' behalf.[9] Many privacy issues are exacerbated by the uninformed use of third-party software components, such as those distributed as software development kits ("SDKs"). Despite the high rates of noncompliance, in the two decades since COPPA became law, an average of two enforcement actions are brought each year.[10] This is largely because regulators are spread too thin: it is simply not feasible for them to open investigations into every conceivable violation, when thousands or more exist.

In many cases, identified privacy issues in child-directed apps and services were not just potential violations of COPPA: many of these issues appeared to violate the posted policies of both the platforms that distributed the apps, as well as other third-party data recipients (i.e., entities distributing SDKs and other components, such as advertising and analytics companies).[11] The authors concluded that these potential violations continue because the policies are rarely enforced. Better guidance to developers from platforms and third-party data recipients would likely prevent many privacy issues, as would proactive enforcement by these entities — particularly of their own publicly posted policies. Unfortunately, these entities are often disincentivized from

[5] 15 U.S.C. § 6502(a)(1).

[6] 15 U.S.C. § 6502(b)(1)(A).

[7] Noura Alomar & Serge Egelman, *Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps*, 2022 PROC. ON PRIV. ENHANCING TECHS. 250, 256.

[8] *See* Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez et al., *"Won't Somebody Think of The Children?" Examining COPPA Compliance at Scale*, PROC. ON PRIV. ENHANCING TECHS., June 2018, at 63, 64.

[9] *See* Alomar et al., *supra* note 7, at 259.

[10] *See Cases Tagged with Children's Online Privacy Protection Act (COPPA)*, FED. TRADE COMM'N., https://www.ftc.gov/enforcement/cases-proceedings/terms/875 [https://perma.cc/8A38-AC9G].

[11] *See, e.g.*, Reyes et al., *supra* note 8, at 75.

acting, despite being in the best position to do so. As a result, individual software developers are burdened with compliance efforts and consumers are burdened with determining which apps and services are privacy-protective, despite neither group being equipped to do so.

Based on these observations and others, effective privacy enforcement should incorporate the following recommendations:

(1) **Hold data recipients accountable.** While consumers care about how their personal information is used, most lack the technical skills and tools to make decisions consistent with those preferences.[12] Similarly, individual software developers — who are myriad — do not understand the privacy implications of the code they write or the third-party components they integrate, which creates compliance problems.[13] Yet, the companies best positioned to remediate privacy violations are currently disincentivized from doing so. COPPA's "actual knowledge" standard[14] disincentivizes platforms, data brokers, and privacy-invasive advertising platforms from proactively determining whether their services are being used in ways that defy relevant laws or even their own policies (e.g., publicly posted in privacy policies and/or terms of service), despite having information readily at their disposal that allows them to do so.[15] Future privacy enforcement should shift the burden from consumers and software developers — those least equipped to detect or remediate violations — to the companies distributing the apps and services and/or collecting the data.

(2) **Eliminate unnecessary exemptions.** COPPA allows companies to collect sensitive user data for ambiguously defined "internal operations" purposes,[16] none of which technically require the collection of that data.[17] Thus, future privacy enforcement efforts should focus on incentivizing data minimization practices, as currently required under the General Data Protection Regulation ("GDPR"),[18] with which many companies distributing consumer software are already required to comply.

[12] See *supra* Sections II.B–C.

[13] See *supra* Section II.F.

[14] 15 U.S.C. § 6501(4)(B).

[15] See *supra* Section III.A.

[16] 15 U.S.C. § 6501(4)(A).

[17] See *supra* Section III.B.

[18] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 5(1)(c), 2016 O.J. (L 119) [hereinafter GDPR].

(3) **Incentivize participation in effective certification programs.** COPPA's Safe Harbor certifiers[19] are largely unaccountable and are incentivized to indemnify the worst actors.[20] Those with good privacy practices are not incentivized to participate in these programs.[21] Worse, the technical analysis they use does not appear to be fit for purpose;[22] no common sets of standards are used, and the certification processes do not comport with modern software development practices.[23] Instead, a private right of action should be used in future privacy legislation to incentivize broader participation in industry self-regulatory programs. More companies would submit to having their apps audited against open technical standards set by experts if doing so resulted in indemnification from the threat of class actions. Moreover, a private right of action would ease the Federal Trade Commission's ("FTC's") burden of investigating the operators of every noncompliant service, allowing the FTC to focus its enforcement efforts elsewhere (e.g., on the far-fewer data recipients and industry self-regulatory programs).

(4) **Focus the FTC's enforcement efforts.** Because the FTC does not have the resources to investigate most violations, its efforts should be focused on setting and enforcing technical standards for certification by industry self-regulatory programs.[24] The FTC could solicit complaints about apps that have been inappropriately certified by safe harbor programs (i.e., noncompliant services that have nonetheless been granted indemnity against private litigation). It could also take action against repeat offenders and the far fewer — but much more impactful — platforms and third-party data recipients. Additionally, it could bring enforcement actions against deficient certification programs, which could result

[19] Under COPPA, the FTC is granted rulemaking authority to create a process under which industry self-regulatory programs are empowered to certify child-directed services as being compliant with COPPA, thereby indemnifying those services against FTC enforcement actions. 15 U.S.C. § 6503; 16 C.F.R. § 312.11. While the FTC evaluates each program's submitted guidelines, there is no standard procedure for each program — or anyone else — to evaluate compliance with each program's guidelines. 16 C.F.R. § 312.11. Thus, while these programs' guidelines, as written, might "meet the requirements" of COPPA, 15 U.S.C. § 6503(b)(2), prior research found no correlation between whether a mobile app had been certified by one of these programs and whether it actually appeared to comply with COPPA when tested, Reyes et al., supra note 8.

[20] *See supra* Section II.E.

[21] Benjamin Edelman, *Adverse Selection in Online 'Trust' Certifications and Search Results*, ELEC. COM. RSCH. & APPLICATIONS, JAN.–FEB. 2011, at 17, 19–20.

[22] *See* Reyes et al., *supra* note 8.

[23] *See supra* Section III.C.

[24] *See supra* Section III.D.

> in the loss of indemnification for services certified by those programs. This would create a much stronger incentive structure for data recipients and platforms to proactively enforce their own policies, as well as for safe harbor certification programs to ensure certified apps and services comply with open certification standards that align with the realities of modern software engineering. The potential loss of indemnification from participating in a deficient program would also motivate services to choose the most reputable certification programs.

As states begin to pass their own comprehensive privacy laws, and as Congress debates passage of a comprehensive federal privacy law, lessons can be learned from COPPA's failures in order to shape more effective privacy enforcement going forward. These lessons are applicable not only to improving children's privacy, but also to enforcing the privacy rights of the broader public. While it is obvious to most that children are not equipped to make these sorts of decisions about their online privacy, neither are most adults (despite holding strong privacy preferences). Thus, the burden of determining whether a given online service complies with basic privacy standards can and should be shifted away from individual consumers.

II. BACKGROUND AND RELATED WORK

This Part provides a broad overview of how and why personal information is collected online and how consumers are opposed to these practices yet have very little awareness or control over them. It describes prior research to understand the online tracking ecosystem, including compliance and enforcement efforts. Based on this research, recommendations for how privacy regulation should change are presented in Part III.

A. Overview of Surveillance Capitalism

Contrary to popular belief,[25] the reason why Internet users receive oddly prescient ads is not because their devices are secretly recording all their conversations.[26] Rather, their preferences and interests have

[25] *See* Kim Komando, *You're Not Paranoid: Your Phone Really Is Listening In*, USA TODAY (Dec. 19, 2019), https://www.usatoday.com/story/tech/columnist/2019/12/19/your-smartphone-mobile-device-may-recording-everything-you-say/4403829002/ [https://perma.cc/UFZ2-VM4H].

[26] *See* Tatum Hunter, *Ask Help Desk: No, Your Phone Isn't Listening to Your Conversations. Seriously*, WASH. POST (Nov. 12, 2021), https://www.washingtonpost.com/technology/2021/11/12/phone-audio-targeting-privacy/ [https://perma.cc/G3KD-3C2Q]. Mobile devices

been inferred by sophisticated algorithms that are powered by the collection of personal information. Online and offline activities are tracked, generating data that is then used by algorithms to make predictions about users, young and old alike. This type of online tracking is made possible by "persistent identifiers." An identifier is any piece of information that allows an individual — or device — to be uniquely identified.[27] "Persistent" identifiers are identifiers that tend to not change over time (or do so very infrequently).[28] For example, motor vehicles have persistent identifiers in the form of license plates: a license plate uniquely identifies a vehicle, and vehicles tend to have the same license plates over time. Thus, if someone records all the license plates observed at a particular place over time, they could determine how many times in that period any individual vehicle was there (and by extension, its operator). Similarly, if license plates are recorded at many different locations and that data is combined into a single dataset, one could use that to reconstruct the movements of individual vehicles within that dataset. As can be seen, combining a persistent identifier with information about where that identifier was observed allows a data recipient to reconstruct an individual's activities — what apps they use and what websites they visit. Using this knowledge, one could infer information about their routines, preferences, demographics, and even relations and social connections.

This process is precisely how online tracking occurs. Mobile phones have various identifiers associated with them, including some that cannot be easily changed (e.g., serial numbers, MAC addresses, IMEI numbers).[29] As a mobile phone tends to be carried and used by a single individual, a unique identifier for a mobile phone is consequently a unique identifier for that individual and can therefore be used to collect data about their activities, preferences, and demographics. This type of online tracking is based on data collection that associates persistent identifiers with the time, manner, location, and what apps individuals used. On the web, browsers send websites persistent identifiers

constantly recording and uploading audio data to remote servers would result in depleted battery life and bandwidth overages, both of which would be noticeable to consumers.

[27] *Persistent Identifiers*, U.S. DEP'T TRANSP. https://transportation.libguides.com/persistent_identifiers [https://perma.cc/Z7NW-VRG6].

[28] *Id.*

[29] I focus on mobile phones for several reasons. First, many more consumers own smartphones than desktop computers. RICHARD WIKE, LAURA SILVER, JANELL FETTEROLF, CHRISTINE HUANG, SARAH AUSTIN, LAURA CLANCY ET AL., SOCIAL MEDIA SEEN AS MOSTLY GOOD FOR DEMOCRACY ACROSS MANY NATIONS, BUT U.S. IS A MAJOR OUTLIER 31, 33 (2022). Second, unlike desktop computers (or even laptops), they tend to be on the owner's person at all times. Third, they allow access by third-party apps and services to myriad types of personal information (including sensor data), more so than what is traditionally collected by apps and services running on desktop operating systems.

in the form of cookies[30] and various types of "fingerprints."[31] It is for this reason that persistent identifiers, including those that identify personal devices, are deemed personal information under various existing privacy laws (e.g., the California Consumer Privacy Act ("CCPA"),[32] COPPA, HIPAA, GDPR, and GLBA).[33]

This tracking is commonly used to monetize many online services. Advertisers pay the operators of websites and mobile apps to show specific advertisements to specific users. They do this by inferring individual users' preferences based on data automatically collected from them. This includes the services they use, how they use them, from where they use them, and so forth. In short, online and offline activities are tracked, which allows companies to maintain detailed profiles of individual user behavior, which in turn are used to predict users' interests, preferences, and even demographics. This data has become the backbone of the Internet economy. The collected information may be used to predict a consumer's religion,[34] health conditions,[35] sexual orientation,[36] or political affiliation.[37] Some of this information may be revealed by the phone's location alone, whether that be via fine-grained GPS data or information about nearby WiFi networks and cellular towers;[38] the phone's IP address, which is transmitted with every Internet connection; or even by just the app that is being used (e.g., the mere presence of a gay dating app or a pregnancy-tracking app reveal the user's likely sexual orientation and pregnancy status, respectively).

Yet, online advertisements need not use consumers' personal information. While the behavioral or targeted advertising described in the prior paragraphs relies on collecting personal information to infer users' interests, contextual advertising does not. Contextual advertising

[30] *See Internet Cookies*, FED. TRADE COMM'N, https://www.ftc.gov/policy-notices/privacy-policy/internet-cookies [https://perma.cc/RW5D-BDVE].

[31] *See* Matt Burgess, *The Quiet Way Advertisers Are Tracking Your Browsing*, WIRED (Feb. 26, 2022, 7:00 AM), https://www.wired.com/story/browser-fingerprinting-tracking-explained/ [https://perma.cc/EGW9-TWMZ].

[32] *See* CAL. CIV. CODE § 1798.140(v)(1).

[33] *See, e.g.*, 16 C.F.R. § 314 (2021).

[34] *See, e.g.*, Minh-Thap Nguyen & Ee-Peng Li, *On Predicting Religion Labels in Microblogging Networks*, PROC. 37TH INT'L 2014 ACM SIGIR CONF. ON RSCH. & DEV. INFO. RETRIEVAL 1211, 1211–14 (2014).

[35] *See, e.g.*, Anupam B. Jena, Pinar Karaca-Mandic, Lesley Weaver & Seth A. Seabury, *Predicting New Diagnoses of HIV Infection Using Internet Search Engine Data*, 56 CLINICAL INFECTIOUS DISEASES 1352 (2013).

[36] *See, e.g.*, Carter Jernigan & Behram F.T. Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, 14 FIRST MONDAY 10 (Oct. 5, 2009).

[37] *See e.g.*, Elanor Colleoni, Alessandro Rozza & Adam Arvidsson, *Echo Chamber or Public Sphere? Predicting Political Orientation and Measuring Political Homophily in Twitter Using Big Data*, 64 J. COMMC'N 317, 317–32 (2014).

[38] *See* Marc Fevrier, *How Does Location Work: Sources of Location Data (GPS, Wifi, Cell Tower Triangulation),* GROUNDTRUTH (Mar. 14, 2018), https://help.groundtruth.com/hc/en-us/articles/360000709047-How-Does-Location-Work-Sources-of-location-data-GPS-Wifi-Cell-Tower-Triangulation [https://perma.cc/Y3JV-K86R].

refers to displaying ads based on what the user is doing in the moment: the type of website or online service that the user is currently visiting and not based on previously collected personal information.[39] For example, a mattress review website does not need to collect personal information to know that visitors might be receptive to ads for mattresses or bedding. By definition, contextual advertising does not require the collection of consumers' personal information because it does not rely on the long-term tracking of their online activities. More importantly, a recent empirical study showed that targeted advertising on websites increased publisher revenues by only four percent over contextual advertising.[40]

Beyond advertising, collected personal data is increasingly used for other purposes that are often opaque to consumers, particularly parents. Some online business models rely on the collection of users' personal data for sales to other entities (i.e., without directly showing users ads at the time that the data is collected)[41] or to "get to know" their users so that they can manipulate users into signing up for paid premium services at later points in time.[42] For example, location data collected by apps is frequently resold to other businesses for a wide range of use cases, such as predicting social relations in the physical world,[43] predicting retail sales trends,[44] law enforcement surveillance,[45] and

[39] *See* FED. TRADE COMM'N STAFF REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 55 n.134 (2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework [https://perma.cc/EW82-98EQ].

[40] Veronica Marotta, Vibhanshu Abhishek & Alessandro Acquisti, *Online Tracking and Publishers' Revenues: An Empirical Analysis* (May 2019) (unpublished manuscript), https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf [https://perma.cc/SBQ3-UP8Q]. However, in practice, it's likely that the returns are even less, as the authors did not consider the marginal costs associated with behavioral advertising: maintaining infrastructure to secure personal data and the associated liability and compliance obligations.

[41] For example, some "monetization SDKs" opaquely collect users' location data for future sales to data brokers.

[42] *See, e.g.*, *Optimize Customer Profiling: Best Practices for Utilizing Segments,* INTUIT MAILCHIMP, https://mailchimp.com/resources/customer-profiling/ [https://perma.cc/L3GW-7MCG].

[43] *See* Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals: Threats to American Civil Rights, National Security, and Democracy*, DUKE SANFORD CYBER POL'Y PROGRAM (Apr. 2021), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf [https://perma.cc/S3D7-ESKK].

[44] *See Foot Traffic Data: The Authoritative Guide for Data Buyers and Sellers*, NEUDATA (Feb. 27, 2023), https://www.neudata.co/blogs/foot-traffic-data-the-authoritative-guide-for-data-buyers-and-sellers [https://perma.cc/7FN9-ZFL5].

[45] *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement*, 29 N.C.J. INT'L L. & COM. REG. 595, 596–98 (2003).

political fundraising and advocacy.[46] Furthermore, many marketplaces exist for data brokers to buy and sell this data, which often includes services and datasets specifically to map persistent identifiers to consumers' names, emails, or physical addresses.[47]

B. Consumer Understanding and Preferences

In addition to questionable economic benefits,[48] over half a century of published research on consumer behavior and preferences has demonstrated that consumers are opposed to the type of tracking described in the prior section. For example, in his consumer surveys on public privacy perceptions going back to the 1970s, Alan F. Westin consistently found that a majority of the American public are either "very" or "somewhat" concerned with how their personal information is collected and used by businesses.[49] In 2001, one study found that as many as sixty-four percent of consumers refused to shop online due to privacy concerns.[50] A 2020 Pew Research Center survey found that more than half of Americans have refused to use certain products or services due to privacy concerns.[51] At the same time, as more aspects of daily life have moved online, many consumers in the past two decades have also simply become resigned to having their information used in objectionable ways.[52] A 2019 Pew Research Center consumer

[46] *See* Geoffrey A. Fowler, *How Politicians Target You: 3,000 Data Points on Every Voter, Including Your Phone Number*, WASH. POST (Oct. 27, 2020), https://www.washingtonpost.com/technology/2020/10/27/political-campaign-data-targeting/ [https://perma.cc/J9ZZ-T2AA].

[47] *See, e.g.*, AWS MARKETPLACE, https://aws.amazon.com/marketplace [https://perma.cc/P79A-XW8X]; DATARADE, https://datarade.ai/ [https://perma.cc/JWP6-NERV]; SNOWFLAKE MARKETPLACE https://app.snowflake.com/marketplace/ [https://perma.cc/MX2C-ELZN].

[48] Marotta et al., *supra* note 40.

[49] Ponnurangam Kumaraguru & Lorrie Faith Cranor, *Privacy Indexes: A Survey of Westin's Studies* 16–18 (Carnegie Mellon Univ. Tech. Rep., Working Paper No. CMU-ISRI-5-138, 2005).

[50] Mary J. Culnan, Professor, Bentley College, Remarks at The Challenges of Providing Effective Financial Privacy Notices: The Consumer and Academic Perspective, a panel at Get Noticed: Effective Financial Privacy Notices, an Interagency Public Workshop 44 (Dec. 4, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/interagency-public-workshop-get-noticed-effective-financial-privacy-notices/glbtranscripts.pdf [https://perma.cc/78XB-76VS].

[51] Andrew Perrin, *Half of Americans Have Decided Not to Use a Product or Service Because of Privacy Concerns*, PEW RSCH. CTR. (Aug. 14, 2020), https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/ [https://perma.cc/8GLH-7TEY]; *see, e.g.*, Salvador Rodriguez, *How Facebook Failed to Break into Hardware: The Untold Story of Building 8*, CNBC (Aug. 3, 2019), https://www.cnbc.com/2019/08/02/facebooks-flop-in-hardware-the-untold-story-of-building-8.html [https://perma.cc/7EDD-XC6F] (regarding the success of the Facebook Portal).

[52] *See* Nora A. Draper & Joseph Turow, *The Corporate Cultivation of Digital Resignation*, 21 NEW MEDIA & SOC'Y 1824, 1824–39 (2019).

survey found that sixty-two percent of Americans do not believe it is possible to "go through daily life without companies collecting data about them," seventy-nine percent are very or somewhat concerned about this, and eighty-one percent believe the risks of collecting this data outweigh the benefits.[53]

Worse, new uses for collected data are invented all the time, which means that there is no way of knowing exactly how collected data may be used in the future. Data collected from mobile apps and other online services could end up being used for making major life decisions, such as the extension of credit, employment, school admissions, or even medical care. When this data comes from children, it is even more concerning. Children are unlikely to understand that these data collection practices are happening, nor can they possibly consent to them, despite potentially facing enormous adverse impacts due to future usage of this data.[54] Companies may use this data for manipulative marketing campaigns. Biased and unaccountable algorithms may also use such data to make decisions about a child's future. Outright malicious uses of the data are also possible (e.g., a non-custodial parent using it to track a child's location). It is unlikely that children are aware when they are being manipulated in this manner.[55] But this is not just a problem for children: it is unlikely that many adults are aware of — much less know how to avoid — these practices.[56]

While consumers are overwhelmingly opposed to this type of tracking and the profiling and reselling of their information that such tracking supports — up to eighty-six percent of U.S. consumers do not

[53] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/8FQG-S5QQ].

[54] *See* Danielle Keats Citron & Frank A. Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014); Joanna Redden, *The Harm That Data Do*, SCI. AM. (Nov. 1, 2018), https://www.scientificamerican.com/article/the-harm-that-data-do/ [https://perma.cc/WER6-JMD3]; Joanna Redden, Jessica Brand & Vanessa Terzieva, *Data Harm Record*, DATA JUST. LAB (Aug. 2020), https://datajusticelab.org/data-harm-record/ [https://perma.cc/UY9G-FYCJ].

[55] *See* BRIAN L. WILCOX, DALE KUNKEL, JOANNE CANTOR, PETER DOWRICK, SUSAN LINN & EDWARD PALMER, REPORT OF THE APA TASK FORCE ON ADVERTISING AND CHILDREN 30, 60 (2004).

[56] *See* Blase Ur, Pedro G. Leon, Lorrie Faith Cranor, Richard Shay & Yang Wang, *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising*, 2012 PROC. EIGHTH SYMP. ON USABLE PRIV. & SEC., July 2012, at 1, 9; Pedro Leon, Blase Ur, Richard Shay, Yang Wang, Rebecca Balebako & Lorrie Faith Cranor, *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*, 2012 PROC. SIGCHI CONF. ON HUM. FACTORS COMPUTING SYS., May 2012, at 589, 593; Sophie C. Boerman, Sanne Kruikemeier & Frederik J. Zuiderveen, *Online Behavioral Advertising: A Literature Review and Research Agenda*, 46 J. ADVERT. 363, 363–64 (2017); Omer Tene & Jules Polenetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281 (2012).

want ads that are tailored based on their online activities[57] — consumers nonetheless continue to engage with services that appear to conflict with their stated privacy preferences. This is known as the "privacy paradox."[58] Industry stakeholders like to use this disconnect to disingenuously claim that it means that consumers do not "really" care about privacy.[59] But the published research on the privacy paradox demonstrates that this is a specious argument because there are several rational explanations for the privacy paradox, including lack of awareness, poor usability, mismatched incentives, and perceived lack of agency.[60]

In many cases, consumers simply do not understand when they are making decisions that will impact their privacy (but are nonetheless expected to make these decisions on behalf of their children, too). For example, in a series of studies, researchers presented participants with different search engine interfaces, including one that annotated search results with privacy information.[61] Subjects were instructed to use the search engine to buy items from merchants of their choice.[62] While all subjects expressed strong privacy preferences in a survey administered prior to the study, when information about privacy practices was not easily accessible, subjects made purchases from the cheapest merchants.[63] On the other hand, when search results were annotated with privacy ratings, subjects were significantly more likely to make purchases from merchants with more agreeable privacy policies (i.e., better aligned with participants' stated privacy preferences), even paying

[57] JOSEPH TUROW, JENNIFER KING, CHRIS JAY HOOFNAGLE, AMY BLEAKLEY & MICHAEL HENNESSY, AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT (2009), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214 [https://perma.cc/YY2A-LMER].

[58] *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 2 (2021).

[59] *How Much You Violate Privacy Depends on How Much Consumers Will Let You*, IAB AUSTL. (Nov. 12, 2014), https://iabaustralia.com.au/how-much-you-violate-privacy-depends-on-how-much-consumers-will-let-you/ [https://perma.cc/T2WC-85Z4].

[60] *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. LAW REV. 1 (2021); Susanne Barth & Menno D.T. de Jong, *The Privacy Paradox — Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior — A Systematic Literature Review*, 34 TELEMATICS & INFORMATICS 1038, 1050–52 (2017).

[61] *See* Janice Y. Tsai, Serge Egelman, Lorrie Cranor & Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RSCH. 254, 257, 260 (2011); Serge Egelman, Janice Tsai, Lorrie Cranor & Alessandro Acquisti, *Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators*, 2009 PROC. SIGCHI CONF. ON HUM. FACTORS COMPUTING SYS. 319 at 322–24; Julia Gideon, Lorrie Cranor, Serge Egelman & Alessandro Accquisti, *Power Strips, Prophylactics, and Privacy, Oh My*!, 2006 PROC. SECOND SYMP. ON USABLE PRIV. & SEC. 133, 134, 137–38.

[62] Tsai et al., *supra* note 61; Egelman et al., *supra* note 61; Gideon et al., *supra* note 61.

[63] Tsai et al., *supra* note 61; Egelman et al., *supra* note 61; Gideon et al., *supra* note 61. The studies controlled for the pricing of goods and the presence of the indicators themselves (i.e., using a placebo condition — indicators that represented something other than privacy — in addition to a control condition that presented no indicators).

more money out of pocket to do so.[64] These studies demonstrate that people often act in ways that seem contrary to their stated privacy preferences when they are not fully aware of business' privacy practices (e.g., due to the well-documented problems with the "notice and consent" framework, under which consumers are expected to read and understand privacy policies).

In other cases, convoluted user interfaces make it difficult for consumers to understand how to make privacy-protective decisions. This poor usability often results in consumers sharing personal information without ever being aware of it. For example, while studies have shown that consumers have concerns about sharing personal information with the wrong audiences on social media, some nonetheless continue to overshare.[65] These actions are the result of difficult-to-use privacy settings interfaces (or mismatches between the design of those interfaces and users' mental models).[66] One early study on the use of Facebook found that, while participants expressed strong privacy preferences, they nonetheless shared sensitive information because more than one in five participants did not understand Facebook's privacy settings or how to use them.[67] Consistent with this finding, the researchers also found that users did not change these settings from the overly-permissive defaults.[68] In a study of file-sharing software, researchers discovered that, due to convoluted privacy settings interfaces, many users were inadvertently sharing their entire hard drives.[69] In a study of tools provided by the advertising industry to opt out of behavioral advertising on websites, researchers observed that "participants found many tools difficult to configure, and tools' default settings were often minimally protective."[70] They also found that, "[w]ithout being familiar with many advertising companies and tracking technologies, it was difficult for participants to use the tools effectively."[71]

Incentives are also important when studying privacy tradeoffs. Privacy decisions are not made in a vacuum. Consumers' engagement with services that violate their privacy preferences is often an indictment of the lack of market choice and an indication of the presence of information asymmetries, rather than an indication that consumers are

[64] Tsai et al., *supra* note 61; Egelman, *supra* note 61; Gideon et al., *supra* note 61.

[65] *See* Maritza Johnson, Serge Egelman & Steven M. Bellovin, *Facebook and Privacy: It's Complicated*, PROC. EIGHTH SYMP. ON USABLE PRIV. & SEC., July 2012, at 1, 10.

[66] *See* Jennifer King, Airi Lampinen & Alex Smolen, *Privacy: Is There an App for That?*, PROC. SEVENTH SYMP. ON USABLE PRIV. & SEC., July 2011, at 1, 9–10.

[67] *See* Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, *in* PRIVACY ENHANCING TECHNOLOGIES: 6TH INTERNATIONAL WORKSHOP 36, 53 (George Danezis & Philippe Golle eds., 2006).

[68] *Id.*

[69] Nathaniel S. Good & Aaron Krekelberg, *Usability and Privacy: A Study of KaZaA P2P File-Sharing*, 2003 PROC. SIGCHI CONF. ON HUM. FACTORS COMPUTING SYS. 137, 138.

[70] Ur et al., *supra* note 56, at 589.

[71] *Id.*

behaving hypocritically.[72] Similarly, privacy is often not the only consideration. If the costs of protecting one's privacy (e.g., time invested learning to correctly use privacy settings, monetary costs, abstaining from social life) are unreasonably high, many consumers will engage with privacy-violative services because they cannot afford the alternatives. For example, when faced with the choice between protecting their privacy or engaging with their peers online, many younger people will choose the latter despite the known privacy risks. Studies have shown that, despite the known privacy risks, many young people continue to use social media due to the fear of missing out,[73] sometimes with the support of their parents (in violation of posted platform policies).[74]

Finally, many consumers simply do not believe they have agency when it comes to making online privacy decisions.[75] Because many believe that their privacy preferences will not be honored no matter the actions they take, many choose to engage with privacy-violative services to extract benefits, believing that they will end up paying the privacy costs regardless.[76] A 2015 consumer survey concluded that, "rather than feeling able to make choices, Americans believe it is futile to manage what companies can learn about them."[77] Similarly, consumers continue to use apps that they find "creepy" due to a sense of learned helplessness — they do not believe that they have the power to control who receives their personal information when they participate in the digital economy.[78]

[72] For example, if one is concerned about Facebook's privacy practices, there is no choice to use a privacy-protective competitor that provides the same benefits.

[73] *See* Vittoria Franchina, Mariek Vanden Abeele, Antonius J. van Rooij, Gianluca Lo Coco & Lieven De Marez, *Fear of Missing Out as a Predictor of Problematic Social Media Use and Phubbing Behavior Among Flemish Adolescents*, 15 INT'L J. ENV'T RSCH. & PUB. HEALTH 589, 589–90 (2018); Dmitri Rozgonjuk, Cornelia Sindermann, Jon D. Elhai & Christian Montag, *Fear of Missing Out (FoMO) and Social Media's Impact on Daily-Life and Productivity at Work: Do WhatsApp, Facebook, Instagram, and Snapchat Use Disorders Mediate that Association?*, ADDICTIVE BEHAV., Nov. 2020, at 110; Ine Beyens, Eline Frison & Steven Eggermont, *"I Don't Want to Miss a Thing": Adolescents' Fear of Missing Out and Its Relationship to Adolescents' Social Needs, Facebook Use, and Facebook Related Stress*, 64 COMPS. HUM. BEHAV. 1, 1–2 (2016).

[74] danah boyd, Eszter Hargittai, Jason Schultz & John Palfrey, *Why Parents Help Their Children Lie to Facebook About Age: Unintended Consequences of the 'Children's Online Privacy Protection Act,'* FIRST MONDAY (2011), https://firstmonday.org/ojs/index.php/fm/article/view/3850/3075 [https://perma.cc/HF9A-VMZX].

[75] Draper & Turow, *supra* note 52, at 2.

[76] *Id.*

[77] JOSEPH TUROW, MICHAEL HENNESSY & NORA DRAPER, THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION 3 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820060 [https://perma.cc/6UNS-W4BY].

[78] *See* Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir & Höskuldur Borghorsson, *Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use*, 2014 PROC. SIGCHI CONF. ON HUM. FACTORS COMPUTING SYS., 2347, 2354–55.

C. Inadequate Privacy Protection Tools

Despite current legal frameworks forcing consumers to bear most of the responsibility for managing their online privacy, consumers are given few tools to do so. Since the dawn of the Internet age, the primary framework for managing online privacy has been "notice and consent," whereby online services post privacy policies ("notice") and consumers can choose whether to engage with services based on their understandings of those policies ("consent").[79] Unfortunately, this framework is fundamentally detached from reality. Decades of research have demonstrated that consumers do not read these privacy policies and, when they do read them, do not understand what they mean.[80] Even worse, privacy policies often do not accurately describe their services' behaviors.[81] For example, one study found that privacy-concerned users were influenced by the mere presence of a privacy policy link, despite few reading the actual policies.[82] This suggests that to many, the mere presence of a privacy policy erroneously signals "good" privacy practices.

If users do opt to read privacy policies, they often must make a significant time investment. In 2008, McDonald and Cranor showed that if users read the privacy policies for every website they accessed, they would need to spend up to three hundred hours per year doing so.[83] Today, the number of websites has proliferated, as has the amount of time that consumers spend online,[84] which suggest that the time investment to read and understand privacy policies has only increased. Though it is unclear whether the time investment to read privacy policies is worthwhile for most consumers, several studies have shown that the privacy policies found on popular websites are written at the college

[79] *See, e.g.*, FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 15–17 (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [https://perma.cc/WSK2-TYTM].

[80] *See, e.g.*, Carlos Jensen & Colin Potts, *Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices*, PROC. SIGCHI CONF. ON HUM. FACTORS IN COMPUT. SYS. 471, 475–77 (2004); Joel R. Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T. Graves et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 41–42, 83–85 (2015).

[81] Benjamin Andow, Samin Yaseer Mahmud, Wenyu Wang, Justin Whitaker, William Enck, Bradley Reaves et al., *PolicyLint: Investigating Internal Privacy Policy Contradictions on Google Play*, PROC. 28TH USENIX SEC. SYMP. 585, 594–96 (2019).

[82] Carlos Jensen, Colin Potts & Christian Jensen, *Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior*, 63 INT'L J. HUM.-COMPUT. STUD. 203, 215 (2005).

[83] *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. LAW & POL'Y INFO. SOC'Y 543, 563 (2008).

[84] *See How Many Websites Are There?*, STATISTA (Aug. 6., 2021), https://www.statista.com/chart/19058/number-of-websites-online/ [https://perma.cc/6M2J-TZ8N]; *Percentage of Population Using the Internet in the United States from 2000 to 2023*, STATISTA, https://www.statista.com/statistics/209117/us-internet-penetration/ [https://perma.cc/4PWL-DU4P].

level and therefore may not be understood by a significant proportion of the population, much less children.[85]

Even when policies are noticed, read, and understood, they generally do not explain a service's data practices in sufficient detail for consumers to make informed decisions. For example, despite CCPA[86] and the California Online Privacy Protection Act[87] both requiring that services post privacy policies, there are no requirements that force those services to name the specific third parties with whom they share data; they are required to name only broad categories of data recipients.[88] Even if third parties may have their own data practices documented in their own privacy policies, it is nearly impossible for consumers to inform themselves about those practices when they are unable to locate those additional privacy policies as a result of not knowing the identities of the companies. Similarly, it is nearly impossible for consumers to understand the privacy practices of large companies that offer multiple services. Privacy policies from those companies can be written in a manner that aggregates their practices across all offered services. For example, Google's privacy policy describes their data collection practices across all of their services and does not convey what data may be specifically collected by each of its products (i.e., what data is collected by Google Maps, as opposed to Google Mail, Google Docs, or Google Search).[89] Similarly, Meta's privacy policy amalgamates data collection practices across Facebook, Messenger, Instagram, Business Tools (i.e., data collected from third-party websites and mobile apps that is shared with Meta), and other data collection sources.[90]

In addition to reading privacy policies, there are technologies that consumers can attempt to use to protect their privacy. However, these technologies remain largely ineffective, offering inadequate protection for consumer privacy rights. "Cookies" are data that websites store in consumers' web browsers, which are then transmitted back to websites when visited in the future.[91] This allows a website to recognize a user over time, without the user having to login again (also allowing the

[85] *See* Yuanxiang Li, Walter Stweart, Jake Zhu & Anna Ni, *Online Privacy Policy of the Thirty Dow Jones Corporations: Compliance with FTC Fair Information Practice Principles and Readability Assessment*, 12 COMMC'N IIMA 65, 83 (2012); Carlos Jensen & Colin Potts, *Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices*, 2004 PROC. SIGCHI CONF. ON HUM. FACTORS COMPUTING SYS. 471, 477; George R. Milne, Mary J. Culnan & Henry Greene, *A Longitudinal Assessment of Online Privacy Notice Readability*, 25 J. PUB. POL'Y & MKTG. 238, 238 (2006).

[86] CAL. CIV. CODE § 1798.130(a)(5)(B).

[87] CAL. BUS. & PROF. § 22575(b)(1).

[88] *See id.*; CAL. CIV. CODE § 1798.130(a)(5)(B).

[89] GOOGLE PRIVACY & TERMS, https://policies.google.com/privacy?hl=en-US [https://perma.cc/Z5EC-S5XD].

[90] Privacy Policy, META, https://www.facebook.com/privacy/policy/ [https://perma.cc/L8SX-HASR].

[91] *What Are Cookies?*, KASPERSKY, https://usa.kaspersky.com/resource-center/definitions/cookies [https://perma.cc/9KPS-DF7M].

website to "remember" other settings, such as a default language). Because cookies have been historically abused for invasive tracking and profiling, modern web browser software allows users to delete stored cookies or to block cookies.[92] However, deleting or blocking cookies is no longer an effective strategy, as tracking now occurs using other means that consumers cannot easily control.[93] For example, unique "fingerprints" — the aggregation of several data points to create a unique identifier — can be constructed based on seemingly-benign information that is automatically transmitted to online services without user consent or knowledge.[94] This information includes sources as diverse as software versions (e.g., the web browser and operating system), language settings, time zones, screen resolution, battery levels, and even installed fonts.[95] Apps on mobile devices have additional data points available for constructing unique fingerprints to identify their users, all without the use of cookies, and with few actions that users can take to prevent tracking from occurring (nor clear understandable indicators to inform them when tracking does occur). Perversely, whether a user has configured privacy settings away from the defaults is often used as a data point for further tracking.[96]

D. Prior Research on COPPA Compliance

As part of prior work on how mobile apps' privacy practices comport with consumers' expectations, researchers wrote bespoke instrumentation for the Android platform, allowing them to run mobile apps and monitor exactly what personal data those apps access and to whom

[92] *See* Jonathan R. Mayer & John C. Mitchell, *Third-Party Web Tracking: Policy and Technology,* 2012 IEEE SYMP. ON SEC. & PRIV. 413, 422–24.

[93] *See* Nick Nikiforakis, Alexandros Kapravelos, Wouter Joosen, Christopher Kruegel, Frank Piessens & Giovanni Vigna, *Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting*, 2013 IEEE SYMP. ON SEC. & PRIV. 541, 542; *see also* Randika Upathilake, Li Yingkun & Ashraf Matrawy, *Classification of Web Browser Fingerprinting Techniques*, 2015 INT'L CONF. ON NEW TECH., MOBILITY & SEC. 1 (taxonomizing web-based fingerprinting techniques).

[94] *See* Upathilake et al., *supra* note 93.

[95] *See* Peter Eckersley, *How Unique Is Your Web Browser?*, *in* 2010 PRIV. ENHANCING TECH. 1, 3–5 (Mikhail J. Atallah & Nicholas J. Hopper eds., 2010); *Learn How Identifiable You Are on the Internet*, AM I UNIQUE, https://amiunique.org/ [https://perma.cc/6PM3-3XYG]; David Fifield & Serge Egelman, *Fingerprinting Web Users Through Font Metrics*, *in* 2015 FIN. CRYPTOGRAPHY & DATA SEC. 107, 108 (Rainer Böhme & Tatsuaki Okamoto eds., 2015).

[96] *See* Geoffrey A. Fowler, *Think You're Anonymous Online? A Third of Popular Websites Are 'Fingerprinting' You*, WASH. POST (Oct. 31, 2019), https://www.washingtonpost.com/technology/2019/10/31/think-youre-anonymous-online-third-popular-websites-are-fingerprinting-you/ [https://perma.cc/NQ7F-5H57]; Michael Simon, *Apple is Removing the Do Not Track Toggle from Safari, but for a Good Reason*, MACWORLD (Feb. 6, 2019), https://www.macworld.com/article/232426/apple-safari-removing-do-not-track.html [https://perma.cc/S6JH-RHVR].

they transmit that data.[97] The tools were written for Google's Android platform because it is open source; Apple's iOS was not examined because the source code is not available to add the same level of instrumentation.[98]

Starting in late 2016, the researchers began downloading as many free apps in the Designed for Families ("DFF") program as they could find, a total of just under 6,000 apps.[99] The DFF program is a section of the Play Store, Google's centralized Android app market, which is exclusively for apps that are directed to children.[100] Mobile app developers must participate in the program when they upload their app and disclose to Google that it is directed at children.[101] As part of the program, they must affirm to Google that their app complies with COPPA.[102] As described below, the researchers observed that many apps did not appear to be complying with COPPA for various reasons.

i. Collection of Contact and Location Information

In terms of the most serious privacy violations, roughly three hundred of the tested apps (4.8%) were observed collecting children's contact information (e.g., names, email addresses, and phone numbers) and/or precise location data.[103] This includes apps specifically targeted at children under the age of five. In most cases, this data was transmitted to third-party advertising companies, or third parties that otherwise support the advertising industry.[104] To put this in perspective, roughly one in twenty of the examined apps were collecting information

[97] Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, & Kohnstantin Beznosov, *Android Permissions Remystified: A Field Study on Contextual Integrity*, 2015 USENIX SEC. SYMP. 499, 501–03; Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner & Konstantin Beznosov, *The Feasability of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences*, 2017 PROC. IEEE SYMP. ON SEC. & PRIV. 1077, 1078, 1080–81; Primal Wijeseker, Joel Reardon, Irwin Reyes, Lynn Tsai, Jung-Wei Chen, Nathan Good et al., *Contextualizing Privacy Decisions for Better Prediction (and Protection)*, PROC. CHI CONF. ON HUM. FACTORS COMP. SYS., Apr. 2018, at 1, 2–4; Joel Reardon, Álvaro Feal, Primal Wijesekera, Amit Elazari Bar On, Narseo Vallina-Rodriguez & Serge Egelman, *50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System*, 2019 USENIX SEC. SYMP. 603, 603.

[98] *See supra* note 97.

[99] Reyes et al., *supra* note 8.

[100] *See* Kanika Sachdeva, *Building a Safer Google Play for Kids*, ANDROID DEVELOPERS BLOG (May 29, 2019), https://android-developers.googleblog.com/2019/05/building-safer-google-play-for-kids.html [https://perma.cc/SN7F-GQG8].

[101] *See* GOOGLE PLAY FAMILY POLICIES, https://support.google.com/googleplay/android-developer/answer/9893335?hl=en [https://perma.cc/7P2G-VV9J].

[102] *Id.*

[103] Reyes et al., *supra* note 8, at 69–73, 76–77.

[104] *Id.* at 70–72, 75–76.

without the requisite verifiable parental consent, a violation for which the FTC has previously brought enforcement actions.[105]

ii. Insecure Transfer of Personal Information

The most common issue observed was the transmission of personal data using insecure means. Under COPPA, covered services must "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[106] While neither the statute nor regulations define what is considered "reasonable procedures," Transport Layer Security ("TLS") and its predecessor have been industry standards for more than three decades now; its use is required on U.S. government websites.[107] Simply put, it is not considered "reasonable" to transmit personal information without the use of TLS to secure it — a view that is shared by the FTC.[108] Nonetheless, the researchers observed that forty percent of the children's apps tested (2,344 apps) failed to take this reasonable precaution.[109] This means that users' personal information was accessible to any eavesdroppers. This may include anyone sharing the same WiFi connection, as well as Internet service providers and other organizations. In an extreme case, this could enable the identification of a specific child within a specific area based on the insecure transmissions emanating from that child's device.

iii. Targeted Advertising

The remaining pervasive privacy issues discovered relate to the collection of persistent identifiers. While a persistent identifier might appear as an insignificant random number or combination of letters, as explained above, persistent identifiers are primarily what enable targeted advertising and other types of user tracking and profiling. The study identified multiple issues. First, Google's user privacy settings may fail to work due to lack of policy enforcement.[110] Second, many app developers fail to correctly configure third-party software components to limit data collection from children, resulting in the sharing of

[105] *See, e.g.*, United States v. Edmodo, LLC, No. 23 Civ. 02495, 2023 WL 3586051 (N.D. Cal. May 22, 2023); United States v. OpenX Technologies, Inc., No. 21 Civ. 09693, 2021 WL 6621824 (C.D. Cal. Dec. 15, 2021); United States v. HyperBeard, Inc., No. 3:20 Civ. 03683 (N.D. Cal. June 3, 2020).

[106] 15 U.S.C. § 6502(b)(2)(D).

[107] *The HTTPS-Only Standard*, U.S. CHIEF INFO. OFFICERS COUNCIL (2015), https://https.cio.gov/ [https://perma.cc/X2RR-ZW4G].

[108] *See* Linda Henry, *FTC Provides Guidance on Reasonable Data Security Practices (Part II of III)*, JD SUPRA (Oct. 18, 2017), https://www.jdsupra.com/legalnews/ftc-provides-guidance-on-reasonable-14614/ [https://perma.cc/HZC8-SNUQ].

[109] Reyes et al., *supra* note 8, at 71.

[110] *See id*. at 77.

children's personal information with third parties for targeted advertising and other prohibited purposes.[111]

E. Ineffective Android Privacy Settings

Prior to 2013, mobile apps for both Google's Android and Apple's iOS mobile operating systems collected a variety of non-resettable identifiers that were used to track consumers.[112] Unlike cookies in the web browser, which can be periodically cleared by the user,[113] many of these identifiers cannot be reset, and so mobile device users have no transparency or control over who is tracking them or when they are being tracked.[114]

In response, both Apple and Google created software-based "advertising identifiers" that could be reset through user-facing privacy controls.[115] By policy, both platforms mandate that only these identifiers be used to track users for advertising and analytics purposes, in lieu of other non-resettable identifiers.[116] This permits consumers to opt out of tracking via a provided settings interface that is supposed to work across all apps installed on the device. However, as was discovered on Android, compliance with this policy did not appear to be proactively enforced by Google: app developers and the third-party mobile SDKs embedded within their apps continue to have the ability to collect non-resettable identifiers alongside resettable advertising IDs.[117] When this happens, if a consumer resets their advertising ID or uses the privacy settings interface to opt out of tracking altogether, data recipients are simply on their honor to stop tracking that consumer.[118] Empirically, despite the adoption of user-facing privacy controls, a significant

[111] *See id.* at 75–76.

[112] Bennett Cyphers, *How to Disable Ad ID Tracking on iOS and Android, and Why You Should Do It Now,* ELEC. FRONTIER FOUND. (May 11, 2022), https://www.eff.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now [https://perma.cc/H6BY-7W6W].

[113] *See* Claire Stouffer, *How to Clear Cookies + Cache in Every Browser*, NORTON (June 13, 2023), https://us.norton.com/blog/how-to/how-to-clear-cookies [https://perma.cc/LW7K-GJKP].

[114] *See The Many Identifiers in Our Pockets*, CITIZEN LAB (May 13, 2015), https://citizenlab.ca/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/ [https://perma.cc/YG4A-6YGU].

[115] *See* Cyphers, *supra* note 112.

[116] *See* Jim Edwards, *Apple Wants More Advertisers to Use Its iPhone Tracking System*, INSIDER (June 13, 2013, 10:17 AM), https://www.businessinsider.com/apples-idfa-and-ifa-tracking-system-2013-6 [https://perma.cc/GQ9E-GW32]; Scott Knaster, *Google Play Services 4.0*, GOOGLE (Oct. 31, 2013), https://developers.googleblog.com/2013/10/google-play-services-40.html [https://perma.cc/CH6F-KX77].

[117] *See* Reyes et al., *supra* note 8, at 75–77.

[118] *See* Irwin Reyes, Primal Wijesekera, Abbas Razaghpanah, Joel Reardon, Narseo Vallina-Rodriguez, Serge Egelman, and Christian Kreibich. *"Is Our Children's Apps Learning?" Automatically Detecting COPPA Violations*, PROC. WORKSHOP ON TECH. & CONSUMER PROT., 2017, at 4.

number of apps continue to use non-resettable identifiers to track users: the researchers observed that thirty-nine percent of the children's apps that were tested transmitted non-resettable identifiers alongside the user-resettable advertising ID.[119] For users of these 2,281 apps, Google's stated platform policies and the devices' systemwide ad privacy settings were simply being ignored by app developers.

i. Ineffective SDK Privacy Settings

Software engineering, like many other types of engineering, involves building products out of many premade components. For example, just as a car manufacturer does not make all the components in its cars, a mobile app developer does not necessarily write all the code found within their apps. Third-party SDKs allow developers to include premade software components, saving them time and effort. For example, rather than find advertisers, create ad copy, and then determine which users to show which ads, app developers can simply outsource that work by incorporating a third-party ad SDK. There are third-party SDKs that help developers with displaying graphics, processing payments, streaming audio or video, and so forth. This type of "code reuse" is an accepted part of modern software engineering.[120] The benefits of this division of labor have been known for centuries.[121] Labor specialization allows organizations to streamline operations by focusing their efforts and preventing time wasted reinventing the wheel. However, integrating third-party components creates enormous risks,[122] especially when app developers fail to verify that those components are functioning as expected (or if third-party components are misused, intentionally or not).

Many of the potential COPPA violations previously observed were due to the data collection behaviors of third-party SDKs, and not necessarily due to code written by app developers themselves.[123] Many of these SDKs, because they are for use in a wide variety of mobile apps,

[119] Reyes et al., *supra* note 8, at 74.

[120] *See* W. B. Frakes & Kyo Kang, *Software Reuse Research: Status and Future*, 31 IEEE TRANSACTIONS ON SOFTWARE ENG'G 529, 529 (2005).

[121] ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS (R.H. Campbell & A.S. Skinner eds., Liberty Classics 1981) (1776).

[122] Third-party components can create both security and privacy risks. Security risks can occur if the component causes the software to behave in dangerous or unexpected ways (e.g., resulting in damage to property, reputation, etc.); privacy risks can occur if sensitive information is inappropriately shared (e.g., in ways that defy an app developer's disclosures or relevant laws/regulations).

[123] The presence of third-party SDKs can be detected by analyzing the application. Additionally, many open source (e.g., EXODUS PRIVACY, https://exodus-privacy.eu.org/en/ [https://perma.cc/S4LE-P5GL]) and commercial products (e.g., APPTOPIA, https://apptopia.com/ [https://perma.cc/QFN6-6GQ5]) provide information about the SDKs found within mobile apps.

offer app developers configuration options so that they can be customized to an app's needs. Specifically, many of the SDKs that collect personal data with COPPA implications — those that may be used to collect personal information from children — offer developers configuration options to enable a COPPA-compliant data-collection mode.[124] When the app developer uses one of these directives to signal that the user is a child, the SDK is instructed to either not use that child's personal information for COPPA-prohibited purposes or not send that data to its servers altogether.[125] When developers of children's apps fail to correctly configure these types of options, their apps may collect children's personal data for targeted advertising and other prohibited purposes.[126]

Few developers were correctly configuring third-party advertising SDKs to disable the collection of personal information for profiling and/or ad targeting purposes.[127] For example, 1,280 of the children's apps tested (21.9%) transmitted users' personal information to Facebook's servers.[128] Of these, only seventy-five (5.9%) correctly signaled to Facebook that the user is a child and that the data should be handled pursuant to COPPA.[129] This also ignores Facebook's explicit instruction that app developers not integrate its SDK into primarily child-directed apps in the first place.[130] Facebook is not an isolated example. Of the third-party SDKs observed collecting personal information while offering options for child-directed treatment, none were consistently configured correctly by app developers.[131] Four years later, another study found that software developers still struggle with this.[132]

Other third-party SDKs simply provided terms of service that prohibited their use in child-directed apps. However, developers of children's apps used these SDKs anyway.[133] By reading the terms of service and privacy policies of these data recipients, the researchers identified several data recipients who (1) described using data received from their SDKs for practices that would be prohibited by COPPA, if that data were to come from children; and (2) prohibited inclusion of their SDKs in child-directed apps. Despite these statements, they

[124] Many SDKs now also offer similar configuration options for newer privacy laws, such as GDPR and CCPA, with research continuing to show that developers do not use these correctly, which leads to privacy compliance issues. *See, e.g.*, Alomar et al., *supra* note 7, at 262.

[125] Reyes et al., *supra* note 8, at 72–73.

[126] *See id.* at 69–70.

[127] *Id.* at 64.

[128] *Id.* at 72.

[129] *Id.*

[130] *See Information for Child-Directed Apps and Services*, FACEBOOK, https://developers.facebook.com/docs/audience-network/optimization/best-practices/coppa/ [https://perma.cc/UD8D-BQKF].

[131] Reyes et al., *supra* note 8, at 72–73.

[132] Alomar et al., *supra* note 7, at 264.

[133] Reyes et al., *supra* note 8, at 71–73.

identified 1,100 children's apps transmitting personal information to these companies (18.8% of the children's apps tested).[134] These transmissions also included information that identified the child-directed apps that were using the SDKs. For example, while ironSource, a behavioral advertising company, posted disclosures with claims of having no knowledge of receiving data from child-directed apps,[135] the researchers pointed out that app developers with names like "BabyBus Kid Games," "For Little Kids," and "GameForKids" were all transmitting data to them for targeted advertising purposes (and that all of these developers would have entered these names when initially signing up to use ironSource's services).[136]

i. Ineffective Industry Certification Programs

Under COPPA, the FTC can indemnify participants in industry self-regulatory programs.[137] That is, once a program is recognized by the FTC, developers of child-directed apps and websites can become certified under that program and receive indemnity from COPPA enforcement actions because they have been deemed compliant with COPPA.[138] As of this date, the FTC's website indicates that six such programs are currently recognized under the COPPA Safe Harbor program.[139] Prior research identified 237 Android apps that gave outward appearances of having been certified as COPPA-compliant by these programs.[140] Yet, when examining the apps' behaviors, the researchers observed that twenty-four apps (10%) collected location data and/or contact information without verifiable parental consent, while seventy-seven (32%) transmitted personal information without taking "reasonable" security precautions (e.g., using TLS encryption).[141] They concluded that apps certified by these programs were just as likely to comply with COPPA as apps not certified by them.[142] Indeed, this finding was consistent with prior research on industry self-regulation, which found that websites receiving trust certifications "are more than twice as likely to be untrustworthy as uncertified sites."[143]

[134] *Id.* at 71.

[135] *Id.* at 82.

[136] Serge Egelman, *We Get Letters*, APPCENSUS BLOG (May 10, 2018), https://blog.appcensus.io/2018/05/10/we-get-letters/ [https://perma.cc/GH4Z-ZPB3].

[137] 15 U.S.C. § 6503.

[138] *Id.*

[139] *COPPA Safe Harbor Program*, FED. TRADE COMM'N., https://www.ftc.gov/safe-harbor-program [https://perma.cc/25YD-2N4B].

[140] Reyes et al., *supra* note 8, at 74–76.

[141] *Id.*

[142] *Id.* at 76.

[143] Edelman, *supra* note 21, at 20.

F. Why Privacy Problems Exist

In more recent work, researchers surveyed and interviewed developers of child-directed mobile apps available both in the United States and Europe.[144] They asked developers whether they were aware of various privacy laws that covered their apps (e.g., GDPR, CCPA, and COPPA).[145] By and large, app developers were aware of these laws and understood that those laws applied to their products.[146] At the same time, most did not have formal processes set up for ensuring — much less monitoring — their compliance with these laws. Instead, many were of the mistaken belief that both Google and Apple perform compliance checking on their behalf.[147] A commonly shared delusion among study participants was that an app would be deemed compliant with all relevant privacy laws simply after it was approved for distribution in the Apple App Store or Google Play Store.[148]

As noted in prior research, most of the observed privacy issues stemmed from data collection performed by third-party components.[149] Many of these third-party components offer specific guidance in their documentation on how to configure them correctly for use in child-directed apps (or apps available in Europe, in the case of GDPR compliance; or apps available to users in California, in the case of CCPA compliance; etc.).[150] In many cases, app developers were simply unaware of these privacy-related configuration options.[151] While the apps were in violation of these third parties' posted terms of service (e.g., by using SDKs that prohibited use in child-directed apps), no proactive enforcement actions appeared to have been taken by these third parties, despite the fact that all of them would have received information identifying the specific apps using their services.

III. Recommendations for Future Enforcement

Several recommendations for improving privacy enforcement follow from the observed problems outlined above. While these observations were made by studying COPPA compliance, these problems are broadly applicable to other privacy legislation, including forthcoming legislation. These recommendations can thus inform the design of future privacy enforcement regimes more generally (i.e., privacy enforcement regimes designed to protect both adults and children). Some of

[144] Alomar et al., *supra* note 7, at 253–54.
[145] *Id.* at 256–58.
[146] *Id.* at 257.
[147] *Id.* at 258–59.
[148] *Id.* at 259.
[149] *See* Reyes et al., *supra* note 8, at 77–78.
[150] *See supra* note 124.
[151] Alomar et al., *supra* note 7, at 254, 263.

these recommendations do not require statutory fixes and can likely be implemented using the FTC's existing authority.

A. Moving from "Actual" to "Constructive" Knowledge

Many of the observed potential violations amounted to sharing persistent identifiers — without verifiable parental consent — with companies whose public disclosures (i.e., privacy policies and/or terms of service) state that those identifiers will be used for activities prohibited by COPPA.[152] These persistent identifiers are generally collected and transmitted by third-party SDKs, and so it is plausible that many app developers simply do not know when this is occurring.[153] However, the third-party data recipients know: in most cases, the information they receive allows them to trivially determine that the transmitting app was directed at children.[154] For example, in correspondence with ironSource, researchers pointed out that all of the observed transmissions identified the name of the app and that app developers additionally disclosed the names of their companies to ironSource as part of the sign-up process.[155]

The privacy policies of many companies that receive personal information from children's apps state they are directed at general audiences, so the companies have "no actual knowledge" of receiving personal information from children, thereby absolving them of any responsibility under COPPA.[156] However, this ignores the fact that each transmission usually includes the name of the app (or website) that transmitted the data.[157] The claim that a third-party data recipient does not have actual knowledge relies on not knowing whether a particular app or service is targeted at children. "Yet, when one looks at the marketing materials of the companies receiving this data, and their business models, it is apparent that this is precisely the type of knowledge that they claim to possess."[158] The advertising and analytics companies that receive this data are specifically in the business of determining the demographics of Internet users based on the services that they use.

Many online advertising business models rely on knowing the demographics of specific apps and websites so that they can target ads

[152] Reyes et al., *supra* note 8, at 71–73.

[153] *Id.*; *see* Alomar et al., *supra* note 7, at 57.

[154] *Protecting Kids Online: Internet Privacy and Manipulative Marketing: Hearing Before the Subcomm. on Consumer Protection, Product Safety, and Data Security*, 117th Cong. 10 (2021) (statement of Serge Egelman, Ph.D., Research Director, Usable Security & Privacy Group International Computer Science Institute) ("[E]ach transmission from an SDK usually includes the name of the app that transmitted the data.").

[155] Egelman, *supra* note 136.

[156] Reyes et al., *supra* note 8, app. at 81–82.

[157] *See id.* at 77.

[158] Egelman, *Protecting Kids Online*, *supra* note 154, at 10.

tailored to those demographics.[159] That is, their internal data allows them to already know or easily find out which online services are child-directed. For data recipients who genuinely do not maintain that data, they can simply query app stores to determine whether an app is child-directed based on its public metadata (e.g., whether it is listed under the "Kids" category of either the Google Play Store or Apple App Store).[160] There are also many commercial offerings for real-time programmatic access to this type of data.[161] But despite the ease with which data recipients could automatically determine whether or not they are receiving data from a child-directed app, data recipients are disincentivized from doing so: a general audience third-party data recipient (e.g., a third-party ad or analytics company) only becomes subject to COPPA when "it has actual knowledge that it is collecting personal information directly from users of another website or online service that is directed to children."[162] Thus, by ignoring the sources of the personal information that they receive, data recipients currently avoid liability under COPPA.[163] As a result, most developers of third-party SDKs place the burden on app developers, rather than using the information that is likely already in their possession — or trivially available to them — to automatically configure their services for COPPA compliance.[164] As previously discussed, many app developers configure these settings incorrectly (or are simply unaware that such settings exist),[165] which results in children being tracked and profiled.

To address these configuration challenges, third-party data recipients should be held to a "constructive knowledge" standard. Under this standard, they would be required to use the information already at their disposal to identify whether the data they receive originates from child-

[159] *See* FED. TRADE COMM'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIOR 2–4 (2009).

[160] This is a trivial task to automate, the lookup could occur in a fraction of a second, and the result could be saved to reduce additional lookups in the future for the same app.

[161] *See, e.g.*, APPTOPIA, https://apptopia.com/ [https://perma.cc/ZYU4-8QFS]; DATA.AI, https://www.data.ai/ [https://perma.cc/8WST-6AJ9]; SENSOR TOWER, https://sensortower.com/ [https://perma.cc/SFD6-T6PD].

[162] FED. TRADE COMN'N, *Complying with COPPA: Frequently Asked Questions*, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions [https://perma.cc/X69W-2CZN].

[163] New Mexico *ex rel.* Balderas v. Tiny Lab Prods., 457 F. Supp. 3d 1103, 1113 (D.N.M. 2020) ("[T]he COPPA Rule reserves liability only for those ad networks with a direct and clear awareness, as opposed to an awareness attributed to them based on what they reasonably should have known, that the apps in which their SDKs are embedded are directed to children."). While this court held — and others have similarly held — that COPPA does not apply to these third parties because the data was communicated to computers and not humans, it ignored the fact that these companies hire humans (i.e., data analysts) to specifically look at the data they receive to improve their services. *Id.* ("The automated transmission of data signals is not an equal substitute for the communication of information in a format that plausibly could impart a direct and clear understanding of that information to the recipient.").

[164] *See supra* note 124.

[165] *See* Alomar et al., *supra* note 7, at 258.

directed services. This would result in not only greater compliance and reduced harm to children, but also drastic cost savings, especially among smaller software development companies and individual entrepreneurs. Moreover, it would incentivize data recipients to actively enforce the terms of their public disclosures (which many consumers may erroneously believe are already being enforced).

A single ad network using its existing data — or data reasonably available to it — to automatically apply child-directed treatment to the data it receives would negate the need for multiple app and website developers to spend time and effort to correctly configure the network's SDK. More materially, a constructive knowledge standard would shift the burden of compliance away from small app developers — who would still need to report whether or not their apps and services are child-directed — to the significantly smaller number of data recipients, who are much better positioned to apply privacy protections to the data that they collect (and are much more likely to do so correctly).[166]

In sum, moving to a constructive knowledge standard would result in fewer incidents of children being inadvertently tracked and profiled. Importantly, this standard should not just apply to protecting children's data; it should also apply to privacy compliance concerning other types of sensitive personal data (e.g., financial and health data). For example, Meta prohibits the use of its tools for the collection of financial and health data,[167] yet routinely receives this type of data from financial- and health-related mobile apps and websites that have integrated Meta's SDKs (alongside information about the websites and apps transmitting said data, which allows them to readily identify those services as health- or financial-related).[168] Meta has also received information about when identifiable patients schedule appointments with hospital websites,[169] as well as information about identifiable users' sexual activity and pregnancy status,[170] despite their posted policies that claim to prohibit companies from sending them health data.[171] Thus, while these public-facing policies are sensible, they are useless without enforcement (whether that be regulatory enforcement or simply data recipients proactively enforcing their own posted policies). The companies setting these policies and receiving the sensitive data are

[166] Ideally, potential data recipients could use this information to apply data minimization principles and prevent this data from being transmitted in the first place (vis-à-vis deleting it from their servers post hoc).

[167] *About Sensitive Health Information*, META, https://www.facebook.com/business/help/361948878201809 [https://perma.cc/A9ZV-RXX4].

[168] *See* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, MARKUP (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites [https://perma.cc/334U-WNS8].

[169] *Id.*

[170] Frasco v. FLO Health, Inc., No. 3 21 Civ. 00757 (N.D. Cal. filed Jan. 29, 2021).

[171] *See* META, *supra* note 167.

best positioned to provide such enforcement. Unfortunately, they currently lack the incentives to perform that enforcement. A constructive knowledge standard would incentivize data recipients and platforms to enforce their stated policies.

B. Eliminating Unnecessary Exemptions

Like all areas of regulation, loopholes may be abused to undermine legislative intent. As written, COPPA provides a loophole regarding the collection of persistent identifiers — the bread and butter of the commercial surveillance industry. Currently, persistent identifiers may be collected from children without parental consent if they are used for the site or service's "internal operations," which the FTC defines as using the data to:

(1) "Maintain or analyze the functioning of the Web site or online service;

(2) Perform network communications;

(3) Authenticate users of, or personalize the content on, the Web site or online service;

(4) Serve contextual advertising on the Web site or online service or cap the frequency of advertising;

(5) Protect the security or integrity of the user, Web site, or online service;

(6) Ensure legal or regulatory compliance; or

(7) Fulfill a request of a child as permitted by § 312.5(c)(3) and (4)" [172]

From a technical standpoint, the collection of persistent identifiers, which allows a user's activities to be tracked between apps (or across websites or other services), is unnecessary for any of these purposes. Each of these use cases could be facilitated by an identifier that is unique to an app installation, web browsing session, or developer, which in turn could not be used to track the user across other apps and services. For example, serving a contextual ad simply requires knowing the type of app or website that a user is using or visiting, which is information that is already collected. By definition, contextual ads are based on that information alone, *not* the user's identity (or observations of their prior behaviors), and therefore do not require the collection of persistent identifiers. Similarly, conversion tracking, measurement, fraud detection, and advertising attribution do not need persistent

[172] 16 C.F.R. § 312.2.

identifiers that can identify users across apps. If they are not performing COPPA-prohibited profiling and behavioral advertising, an advertising company only needs to know how many people clicked on a specific ad, not who those individuals are. When user-specific identifiers are needed, ephemeral app- or session-specific identifiers can be used. This functionality is already supported on both Android and iOS (i.e., the major mobile platforms),[173] as well as within web browsers and on the desktop.[174] Eliminating the internal operations exemption should therefore not create an undue compliance burden.

Furthermore, claims that persistent identifiers are needed for these purposes are disingenuous because many app developers are already prevented by platform policies from using identifiers for many of these purposes. Indeed, on iOS, if a user opts out of online tracking, apps are outright prevented from accessing identifiers that could be used to track that user's behavior across apps.[175] Further, Apple already requires that *no* persistent identifiers can be collected from children's apps.[176] Google recently adopted similar policies for child-directed apps[177] and also provides best practices for developers that explain how ephemeral identifiers can be used to protect user privacy for many of these use cases.[178] Thus, it is false to claim that persistent identifiers are necessary for these purposes.

The FTC has previously advocated for companies to take a "data minimization" approach to online privacy.[179] This advice should be heeded more generally, as is the case under the GDPR.[180] Data that is not strictly needed should simply not be collected. To address this, the FTC could use its rulemaking authority to drastically narrow the definition of "internal operations" and pursue enforcement actions against

[173] *AppSetId*, ANDROID DEVELOPER, https://developer.android.com/design-for-safety/privacy-sandbox/reference/adservices/appsetid/AppSetId [https://perma.cc/H4W5-SANP]; *identifierForVendor*, APPLE DEVELOPER, https://developer.apple.com/documenta tion/uikit/uidevice/1620059-identifierforvendor [https://perma.cc/2NJQ-R8S7].

[174] *See, e.g.*, *uuid — UUID objects according to RFC 4122*, PYTHON, https://docs.python.org/3/library/uuid.html [https://perma.cc/N3NS-K85N]; *Class UUID*, ORACLE, https://docs.oracle.com/javase/8/docs/api/java/util/UUID.html [https://perma.cc/U9EA-67W5]. On both the web and on the desktop, most programming languages allow a developer to generate a random identifier and save it in local storage.

[175] *advertisingIdentifier*, APPLE DEVELOPER, https://developer.apple.com/documenta tion/adsupport/asidentifiermanager/advertisingidentifier [https://perma.cc/WH48-LBUF]

[176] *App Store Review Guidelines*, APPLE, https://developer.apple.com/app-store/review/guidelines/ [https://perma.cc/NA4X-F8SR].

[177] *Data Practices in Families Apps*, GOOGLE, https://support.google.com/googleplay/android-developer/answer/11043825?hl=en [https://perma.cc/8925-FWZG].

[178] *Best Practices for Unique Identifiers*, ANDROID, https://developer.android.com/training/articles/user-data-ids [https://perma.cc/LAN7-9MM7].

[179] *FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks*, FED. TRADE COMM'N. (Jan. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices [https://perma.cc/7JXQ-67EA].

[180] GDPR art. 5 § 1(c).

data collection that occurs for "any other purpose" more aggressively.[181] More broadly, while platforms publicly post policies that prohibit these practices in children's apps, they can expand these policies to cover other apps and services that involve data collected from adult consumers. But as noted before, such policies are effectively useless without proactive enforcement.

C. Creating Effective Certification Programs

While the FTC has brought many successful enforcement actions, it is simply not feasible for FTC employees to investigate every violation, even for violations resulting in consumer concrete harms. Arguably, this is why Congress created the Safe Harbor program that is part of COPPA: to offload some of the enforcement burden to industry self-regulatory programs. Yet, COPPA Safe Harbor programs appear to be largely ineffective because they ignore the realities of modern software development. Apps and websites are certified without sufficient empirical data, and to the extent that they do undergo technical audits, these occur at discrete points in time.[182] These certification processes are thus completely divorced from software release cycles: a product is certified for a period of time based on an incomplete examination of one particular version, whereas subsequent releases may never be examined.

While the certification methodology and procedures are shared with the FTC, they are not made public. Ideally, certification methodologies would follow open standards set by recognized experts. This is applicable not just to COPPA, but also to any future privacy protection regimes that involve industry self-regulation.

Given the poor incentive structures and lack of transparency around how apps are certified, or even around the determination of which apps are certified, current Safe Harbor programs do not appear to be effective. Improvements can be made following three approaches:

(1) Apps and services should be certified based on independent forensic evaluations of their privacy-relevant behaviors.

(2) The FTC should develop, in consultation with privacy experts, open standards for those forensic evaluations. The FTC should focus its enforcement efforts on ensuring that certification programs adhere to these standards.

[181] 15 U.S.C. § 6501(4)(A).

[182] COPPA regulations require only "a comprehensive review by the safe harbor program, to be conducted not less than annually, of each subject operator's information policies, practices, and representations." 16 CFR § 312.11(b)(2).

(3) Certification organizations should be required to publish lists of the apps they have certified (including the specific versions examined and when).

Based on examinations of public documents that describe COPPA Safe Harbor certification processes, it appears as though current certification processes rely primarily on self-reports from software developers, rather than forensic examinations of their apps and services that would actually yield the data necessary to assess compliance.[183] Given that many app developers are unaware of the privacy issues associated with their apps,[184] it would hardly be a surprise that those behaviors do not get disclosed to the certification organizations, resulting in the inadvertent certification of COPPA-violating apps and therefore inappropriate indemnification against FTC enforcement.

Relatedly, simply finding the apps that had been certified by each organization is a difficult task, as many do not publish this information. Researchers reported having difficulty determining which apps had or

[183] *See COPPA Safe Harbor Program*, *supra* note 139. For example, CARU's Safe Harbor status request only makes mention of self-assessment forms and website reviews by CARU staff, whereas no mention is made of how these reviews will be performed from a technical standpoint, nor how they apply to mobile apps. Letter from Wayne J. Keeley, Dir., Children's Advert. Rev. Unit, Advert. Self-Regulatory Council, to Donald S. Clark, Secretary, Fed. Trade Comm'n (2013), https://www.ftc.gov/system/files/attachments/press-releases/revised-childrens-online-privacy-protection-rule-goes-effect-today/130701carusafeharborapp.pdf [https://perma.cc/678M-P3CH]. kidSAFE similarly makes no mention of any sort of technical evaluations. kidSAFE, Certification Rules — Version 3.0 (FINAL), https://www.ftc.gov/system/files/attachments/press-releases/ftc-approves-kidsafe-safe-harbor-program/kidsafe_seal_program_certification_rules_ftc-approved_kidsafe_coppa_guidelines_feb_2014.pdf [https://perma.cc/9QBD-HWJG]. Both ESRB's and PRIVO's applications claim that ongoing monitoring will be performed of certified websites and mobile apps, but no technical details are provided to explain how that will occur. Letter from Dona J. Fraser, Vice President, ESRB Priv. Certified, to Donald S. Clark, Secretary, Fed. Trade Comm'n (June 23, 2013), https://www.ftc.gov/system/files/attachments/press-releases/entertainment-software-rating-board-awarded-safe-harbor-status/sh_130701esrb_application.pdf [https://perma.cc/M3C7-696B]; Letter from Lauren Lynch Flick, Pillsbury Winthrop Shaw Pittman LLP, to Donald S. Clark, Secretary, Fed. Trade Comm'n (June 27, 2013), https://www.ftc.gov/system/files/attachments/press-releases/revised-childrens-online-privacy-protection-rule-goes-effect-today/130701privosafeharbor.pdf [https://perma.cc/4YLF-7VA7]. iKeepSafe's application mentions using an intercepting web proxy to capture data, iKeepSafe, General Statement of Program Requirements, https://www.ftc.gov/system/files/attachments/press-releases/ftc-seeks-public-comment-ikeepsafes-proposed-safe-harbor-program-under-childrens-online-privacy/ikeepsafeprogramapp_0.pdf [https://perma.cc/WEF5-GGWE], but this will not, for example, capture plaintext traffic secured using "certificate pinning" or using QUIC, *see* Jeffrey Walton, John Steven, Jim Manico, Kevin Wall & Ricardo Iramar, *Certificate and Public Key Pinning,* OWASP, https://owasp.org/www-community/controls/Certificate_and_Public_Key_Pinning [https://perma.cc/GR3L-M94X]; Internet Eng'g Task Force, QUIC: A UDP-Based Multiplexed and Secure Transport, https://www.rfc-editor.org/rfc/rfc9000.pdf [https://perma.cc/EDN8-TYEM]. Furthermore, using a web proxy to capture traffic from an Android app requires modifying the app to specifically allow it. *See Network Security Configuration*, Android Developers, https://developer.android.com/privacy-and-security/security-config [https://perma.cc/NC5H-ZZLP].

[184] Alomar et al., *supra* note 7, at 258.

had not been certified by each program.[185] It is therefore hard to expect more of the average parent. Mandates to make this information public, in an accessible manner, would not only empower parents to make better decisions, but also strengthen the free market through increased transparency, thereby promoting competition.

At the same time, participation in certification needs to be incentivized. Currently, participation in the COPPA Safe Harbor programs is incentivized by indemnifying companies against FTC enforcement. But if FTC enforcement is rare to nonexistent as a proportion of total potential violations, this is a paper tiger. (Nonetheless, prior work has shown that selective enforcement is somewhat of a deterrent, particularly among large organizations that have the resources to invest in dedicated compliance personnel.)[186] Instead, the threat of enforcement needs to be more credible: in surveys of developers, researchers observed that the threat of being removed from app stores is a significantly more credible threat than the threat of enforcement from regulatory agencies.[187] At the same time, plaintiffs' attorneys are routinely examining the digital ecosystem to identify bad actors and bring many more cases than regulators (largely because there are many more of them and they are better resourced).[188] This dynamic can be leveraged to incentivize participation in robust certification programs. Future privacy laws should include a private right of action and can then use indemnification against it as an incentive to participate in certification programs.

These recommendations apply generally, well beyond COPPA. In other words, future comprehensive privacy laws that offer similar safe harbor programs should use indemnification against a private right of action as a participation incentive. It is unrealistic to expect a single agency to be responsible for investigating all privacy violations across multiple industries. This has not been effective for COPPA enforcement, and it is unlikely to be effective for state privacy laws, much less federally under future comprehensive privacy laws. Part of this responsibility can be offloaded through certification programs as outlined above. But for these programs to be effective, they must be designed to avoid adverse selection problems, in which only the worst actors are

[185] *See, e.g.*, Reyes et al., *supra* note 8, at 75.

[186] Kenneth Bamberger & Deirdre Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 261–63 (2011).

[187] Alomar et al., *supra* note 7, at 259.

[188] *See, e.g.*, Emily Kesler, *A Recent Surge of Consumer Privacy Litigation Asserting Violations of the Video Privacy Protection Act (VPPA) Seeks to Hold Companies Liable for Data Sharing in Context of Marketing Analytics*, CONSUMER CLASS DEF. BLOG (Jan. 25, 2023), https://www.consumerclassdefense.com/2023/01/a-recent-surge-of-consumer-privacy-litigation-asserting-violations-of-the-video-privacy-protection-act-vppa-seeks-to-hold-companies-liable-for-data-sharing-in-context-of-marketing-analytics/ [https://perma.cc/7992-U837].

incentivized to participate.[189] Certification programs must also follow reasonable technical standards set by independent experts.

D. Focusing Enforcement Efforts

With a robust self-regulatory program that has strong incentivizes for participation (i.e., indemnification from class actions), the FTC can focus its efforts on policing the certification programs, rather than the myriad of more individual services. The FTC (or another agency or appointed group) could establish open standards for these programs and ensure adherence to those standards. Separately, the FTC could also use its existing authority to incentivize more proactive enforcement among platforms and third-party data recipients.

i. Effective Industry Certification Programs

Specific technical standards used to certify services as compliant (and thereby indemnifying them from private enforcement) could be developed by an appointed committee of recognized experts in conjunction with public comment processes. Alternatively, the development of standards could be delegated to another agency, such as the National Institute of Standards and Technology. The resulting certification standards should be specific and made publicly available.

One concern with allowing industry certification programs that impart indemnity is the inappropriate certification of deficient apps and services (as is currently a problem under COPPA). While some deficient services might receive indemnity under a certification program, the FTC could solicit reports of deficient services — potentially by offering “bug bounties” paid out of bonds posted by approved certification programs or from fines levied against offenders.[190] The FTC could then focus its enforcement efforts on the certification programs responsible (e.g., after receiving multiple reports related to a single certification program), including revoking the status of certification programs that are deemed repeat offenders. If a certification program loses its status, this could remove the indemnification status of all previously certified apps and services (e.g., if they fail to get certified by another program within a certain grace period). In turn, this would incentivize individual software developers to seek certifications from higher quality certification programs (i.e., those unlikely to lose their certification status due to FTC enforcement actions).

[189] Edelman, *supra* note 21.

[190] *What Are Bug Bounties? How Do They Work? [With Examples]*, HACKERONE (July 16, 2021), https://www.hackerone.com/vulnerability-management/what-are-bug-bounties-how-do-they-work-examples [https://perma.cc/KNP8-W5XJ].

This incentive structure, in turn, would serve as motivation for certification programs to rigorously enforce their own standards. Faced with the prospect of losing their ability to certify apps and services, certification programs will be motivated to adhere to their own standards during the certification process and investigate reports of noncompliance among the apps and services that they certify.

Of course, this framework can only work if there is a real threat of enforcement. Apps and services would be incentivized to participate in certification programs due to the threat of enforcement actions brought by the plaintiffs' bar. Due to the threat of FTC enforcement actions, certification programs are incentivized to rigorously apply prescribed open standards set by experts and investigate and remediate reports of noncompliance. Thus, a private right of action is necessary to create the right incentive structure for industry certification programs to be effective.

ii. Incentivizing Proactive Policy Enforcement

While creating a private right of action requires statutory changes, the FTC can take actions using its existing authority under the FTC Act[191] to maximize its own enforcement efforts. As noted earlier, many potential COPPA violations also violate the posted policies of the platforms distributing the mobile apps, as well as those of third-party data recipients (e.g., advertising networks, analytics companies, and data brokers). For example, compliance with many of COPPA's provisions is already required in the platform policies of both Google and Apple,[192] and advertisers like Meta forbid developers from using their services to collect data from children or certain types of sensitive data from adults (e.g., health and financial data).[193] A reasonable person reading these policies would assume that these companies are therefore not collecting this data (and certainly not using it for secondary purposes, such as ad targeting, other user profiling, sales to data brokers, etc.). But without proactive enforcement, that is simply not the case. Thus, an argument could be made that by posting these disclosures and doing nothing to enforce them, consumers are being deceived about the level of privacy protections afforded to them.

As a result, the FTC may be able to use its Section 5 authority to pursue enforcement actions against platforms and large data recipients who post unenforced policies that result in the surreptitious collection of consumer data en masse (and thus materially deceive consumers

[191] 15 U.S.C. § 45 *et seq*.

[192] GOOGLE, *supra* note 177; APPLE, *supra* note 176.

[193] META, *supra* note 167; MARKUP, *supra* note 168.

about the privacy protections that they are receiving).[194] This could result in two possible positive outcomes. First, and most ideally, it would prompt these entities to begin proactively enforcing their own policies across the millions of software developers who use their services. This would allow the FTC to focus and maximize its enforcement activities, as previously described. Alternatively, it may cause these entities to revise their public disclosures to better match reality. While the latter is a less desirable outcome from a consumer privacy standpoint, it would nevertheless allow both consumers and software developers to make more informed choices about the services they use (and the levels of privacy afforded by them).

IV. CONCLUSION

Prior research has shown how COPPA compliance and enforcement have been failing, resulting in the inappropriate collection of personal information from child-directed online services. In one study, researchers found that a majority of 5,855 child-directed Android apps appeared to be violating COPPA in various ways.[195] They found that many of the identified issues were due to developers' incorrect use of third-party software components (i.e., advertising and analytics SDKs) and that self-regulatory Safe Harbor programs had no observable effect on apps' rates of compliance.[196] Subsequent research involving surveys and interviews with app developers found that app developers are often legitimately unaware that these issues exist in their apps, or that they are due to unexpected and/or undocumented behaviors caused by the third-party components that they use.[197] Many developers were of the erroneous belief that app distribution platforms were conducting compliance checks on their behalf.[198] While the aforementioned research focused on children's privacy, the lessons learned should also be applied towards improving privacy enforcement for people of all ages.

[194] *See* 15 U.S.C. § 45; *see also A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/mission/enforcement-authority [https://perma.cc/E33V-JVJC] (describing the FTC's authority to prevent "unfair or deceptive acts or practices" under 15 U.S.C. § 45(a)(1)). The practice of posting unenforced policies may be deceptive (i.e., the disclosures may materially mislead a reasonable consumer into believing they are receiving greater privacy protections), but it also may be unfair.

[195] Reyes et al., *supra* note 8, at 69.

[196] *Id.* at 74–76.

[197] *See* Alomar et al., *supra* note 7, at 258.

[198] *Id.* at 259 ("'[I]f my app is not complying with COPPA, GDPR or the Google Play policies, then my apps should not be on the store. I am not liable because Google is checking and so the responsibility is on Google.' . . . 'I can confidently say that all my apps are compliant with all the standards because it was verified by Google before they published it.'").

Because of developers' apparent lack of awareness,[199] simply informing developers of common privacy issues, and the fact that they are associated with legal jeopardy, could be a powerful first step towards remediation. Many app developers already look to platforms for this guidance; app developers are much more concerned with the threat of being removed from the app stores than the threat of regulatory enforcement.[200] As a result, platforms are best positioned to provide guidance on compliance to developers, and developers are much more likely to act on that guidance.[201] Similarly, third parties receiving the data often have enough information at their disposal to automatically detect when their services are being misused in ways that violate their own policies and relevant laws.[202] Thus, the absence of misuse detection is due to misaligned incentives.

To provide some of these incentives while also maximizing limited public resources, the FTC's enforcement efforts should be focused on ensuring that the data recipients and platforms are enforcing their own stated policies (since there are fewer data recipients and platforms than developers, as well as eliminating regulatory loopholes through new rulemaking. Of course, statutory fixes are still needed to correctly incentivize participation in (and the effectiveness of) industry self-regulatory certification programs. A private right of action is therefore needed to create those incentives. Participation in self-regulatory programs can be incentivized by indemnification from civil liability, allowing the FTC to focus its resources on ensuring that these programs follow open standards set by experts. Such an enforcement regime would promote both competition and transparency, while also relieving individual developers and consumers of their current burden of being forced to identify which services are actually protective of consumer privacy — a burden that most are ill-equipped to correctly undertake.

[199] *See supra* Section II.F.

[200] *See* Alomar et al., *supra* note 7, at 258.

[201] Platforms could provide an overview of the privacy laws that may apply, tips for complying, and common mistakes. Privacy-relevant configuration information for common SDKs could also be made available (including links to documentation on SDK developers' websites).

[202] *See supra* Section III.A.