AGE-APPROPRIATE DESIGN CODE MANDATES

STACY-ANN ELVY*

ABSTRACT

Fueled by the Internet of Things and various other technological developments, information about children's daily activities and social interactions are progressively migrating to the digital sphere. In response to the rapid datafication of children and in accordance with the United Kingdom's Data Protection Act of 2018, the Information Commissioner's Office issued the Age-Appropriate Design Code ("U.K. Design Code"), which became enforceable in September 2021. Approximately one year later in September 2022, California enacted the California Age-Appropriate Design Code Act ("California Design Act"). The California Design Act is modeled after the U.K. Design Code. This Article is one of the first legal scholarship to comparatively analyze in-depth the California Design Act and the U.K. Design Code. This Article advances current privacy law and comparative law scholarly literature by shedding light on relatively substantive similarities and differences between the U.K. Design Code and the California Design Act while conducting a broader field of inquiry that offers potential reasons for the notable differences between both frameworks. The Article also simultaneously conducts a detailed evaluation of the California Design Act's potential to protect children's privacy in the modern era in light of the federal Children's Online Privacy Protection Act

* Professor of Law and Martin Luther King Jr. Hall Research Scholar, University of California, Davis School of Law (J.D., Harvard Law School; B.S., Cornell University). For helpful feedback, conversations, comments or insights, I am grateful to Margot Kaminski, Ashutosh Bhagwat, Cedric Powell, Tom Kemp and to the other participants at the University of Colorado Law School Faculty Colloquium. I am also grateful to my research assistant, Nicholas Takton, for his help with this project.

of 1998. Children's online and traditional offline daily actions are increasingly monitored and monetized. The Article concludes by offering a path forward to better safeguard children's privacy in the United States.

TABLE OF CONTENTS

INTRODUCTION

With the dawn of the United Kingdom's Age-Appropriate Design Code ("U.K. Design Code"), which became enforceable in September 2021 after the end of a twelve-month compliance grace period, the United Kingdom positioned itself as a leader on children's privacy.[1] The U.K. Design Code received praise from its advocates as the first "code of practice for children's data anywhere in the world."[2] In response to the U.K. Design Code, YouTube made "uploads private by default" for children between the ages of thirteen to seventeen so that only approved followers can view children's videos and "turned off auto-play by default for minors."[3] Instagram and TikTok followed suit by making children's profiles private by default and limiting strangers' ability to interact online

---

[1] U.K. INFORMATION COMM'N'S OFF., AGE APPROPRIATE DESIGN: A CODE OF PRACTICE FOR ONLINE SERVICES (2020), https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf [https://perma.cc/HXM2-3U5T] [hereinafter U.K. Design Code]; IRELAND DATA PROTECTION COMM'N, FUNDAMENTALS FOR A CHILD-ORIENTED APPROACH TO DATA PROCESSING (2021), https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf [https://perma.cc/BE4Q-TPA7]; Adele Harrison, *The UK's Age-Appropriate Design Code Comes into Force in September 2021*, JD SUPRA (July 27, 2021), https://www.jdsupra.com/legalnews/the-uk-s-age-appropriate-design-code-5772164/ [https://perma.cc/EWQ3-C8SF]; Natasha Lomas, *UK Now Expects Compliance with Children's Privacy Design Code*, TECHCRUNCH (Sept. 1, 2021), https://techcrunch.com/2021/09/01/uk-now-expects-compliance-with-its-child-privacy-design-code/ [https://perma.cc/367U-DQFB].

[2] *Age Appropriate Design Code*, 5 RTS. FOUND., https://5rightsfoundation.com/our-work/design-of-service/age-appropriate-design-code.html [https://perma.cc/QPZ4-T7H8] (last visited Oct. 12, 2022).

[3] Natasha Singer, *Sweeping Children's Online Safety Bill Is Passed in California*, N.Y. TIMES (Aug. 30, 2022), https://www.nytimes.com/2022/08/30/business/california-children-online-safety.html [https://perma.cc/4NMC-PAS5]; *see also Google Announcement Shows Impact of Children's Code*, 5 RTS. FOUND. (Aug. 10, 2021), https://5rightsfoundation.com/in-action/google-announcement-shows-impact-of-childrens-code.html [https://perma.cc/33LT-3JC4] ("They will turn off auto-play on YouTube giving kids a chance to make a choice to watch (or not) the next video instead of automating attention.").

with young children.[4] Google also disabled its location history feature for children in response to the U.K. Design Code.[5]

Approximately one year later in September 2022, California enacted the California Age-Appropriate Design Code Act ("California Design Act"), which was initially scheduled to become operative on July 1, 2024.[6] A few months after the California Design Act's passage, an industry trade association challenged the statute's legal validity, a dispute that is still ongoing at the time of this writing.[7] In "the uncodified preamble of the bill that enacted"[8] the California Design Act, the California legislature encouraged corporate actors and the newly established working group to follow U.K. guidance flowing from the U.K. Design Code when designing and developing services and products for children subject to the

---

[4] Ben Brody, *The UK Finally Got Big Tech to Boost Teens' Privacy*, PROTOCOL (Aug. 13, 2021), https://www.protocol.com/amp/tiktok-google-facebook-aadc-2654657705 [https://perma.cc/L6FG-U7NB]; Singer, *supra* note 3.

[5] Singer, *supra* note 3.

[6] Assembly B. 2273, 2021-2022 Gen. Assembly, Reg. Sess. (Cal. 2022) (enacted); Natasha Singer, *California Governor Signs Sweeping Children's Online Safety Bill*, N.Y. TIMES (Sept. 15, 2022), https://www.nytimes.com/2022/09/15/business/newsom-california-children-online-safety.html [https://perma.cc/XFE5-GGZJ]; Press Release, Gavin Newsom, Governor, State of California, Governor Newsom Signs First-in-Nation Bill Protecting Children's Online Data and Privacy (Sept. 15, 2022), https://www.gov.ca.gov/2022/09/15/governor-newsom-signs-first-in-nation-bill-protecting-childrens-online-data-and-privacy/ [https://perma.cc/RM5Y-MBLB].

[7] Order Granting Motion for Preliminary Injunction, Netchoice v. Bonta, No. 5:22-cv-8861, 2023 WL 6135551 (N.D. Cal. Sept. 18, 2023), ECF No. 74 (granting a preliminary injunction against the California Age Appropriate Design Code Act); Notice of Preliminary Injunction Appeal, Netchoice v. Bonta, No. 5:22-cv-8861-BLF (N.D. Cal. Oct. 18, 2023), ECF No. 75 (appeal to the Ninth Circuit Court of Appeals of the district court's preliminary injunction); Press Release, Attorney General Bonta Files Notice of Appeal to Overturn Preliminary Injunction Blocking Children's Online Safety Law (Oct. 18, 2023), https://oag.ca.gov/news/press-releases/attorney-general-bonta-files-notice-appeal-overturn-preliminary-injunction [https://perma.cc/ZUN3-4V3H] (reporting that the California Attorney General has "filed a notice of appeal to overturn a preliminary injunction that would block . . . the California Age-Appropriate Design Code Act . . . from going into effect"); Lauren Berg, *Calif. Internet Law Does More Harm Than Good, Big Tech Says*, LAW360 (Dec. 14, 2022), https://www.law360.com/cybersecurity-privacy/articles/1558473 [https://perma.cc/MW5J-L5TQ] (discussing the 2022 lawsuit challenging the constitutionality of the California Design Act).

[8] Judd v. Weinstein, No. CV-18-5724 PSG (FFMx), 2019 U.S. Dist. LEXIS 42238, at *16 (C.D. Cal. 2019).

California Design Act.[9] This push to follow U.K. guidance appears to be an attempt to foster transatlantic privacy law cooperation and harmonization, ideals enabled, in part, by collaborative governance. Other states, such as Oregon and New Jersey, proposed laws modeled after the California Design Act.[10]

This Article is one of the first legal scholarship to both comparatively analyze in-depth the California Design Act and the U.K. Design Code and evaluate the ability of the California Design Act to protect children's privacy in the modern era. While acknowledging differences between the legal systems in the United Kingdom and the United States, this Article advances current privacy law and comparative law scholarly literature by shedding light on relatively substantive similarities and differences between the U.K. Design Code and the California Design Act with a primary focus on evaluating the potential of the California Design Act to ameliorate the various child privacy concerns highlighted in this Article. The Article offers potential reasons for the notable

---

[9] Cal. Assembly B. 2273 § 1(d) ("It is the intent of the Legislature that businesses covered by the California Age-Appropriate Design Code may look to guidance and innovation in response to the Age-Appropriate Design Code established in the United Kingdom when developing online services, products, or features likely to be accessed by children."). Courts may rely on the uncodified preamble of a bill that enacted a statute to determine legislative intent and in conducting statutory analysis. *See, e.g.*, *Weinstein*, 2019 U.S. Dist. LEXIS 42238, at *15-17 (analyzing the preamble to California Civil Code Section 51.9, which discusses sexual harassment in professional relationships, to determine statutory coverage); McClung v. Emp. Dev. Dep't., 34 Cal. 4th 467 (2004) (A "'legislative declaration of an existing statute's meaning' is . . . a factor for a court to consider [but] is 'neither binding nor conclusive in construing the statute.'" (citing W. Sec. Bank v. Sup. Ct., 34 Cal. 4th 467 (1997))). The seeming encouragement of reliance on U.K. Design Code guidance could also be due to potential limitations on the adoption of informal guidance as opposed to formal regulations as defined in the California Administrative Procedure Act. *See generally* CAL. GOV. CODE §11340 et seq. (West 1993); OFF. OF ADMIN. LAW, GUIDE TO PUBLIC PARTICIPATION IN THE REGULATORY PROCESS 1 (2017), http://www.cgcc.ca.gov/documents/enabling/2017/How-2-Participate-102016.pdf [https://perma.cc/J6SZ-KJ8A] ("Unless expressly exempted, state agencies must follow the procedures and requirements set forth in the California Administrative Procedure Act (Government Code § 11340 *et seq*.) (APA) and rules adopted by the Office of Administrative Law (OAL)."); Jonathan Wood, *Underground Environmental Regulations: Regulations Imposed As Mitigation Measures Under CEQA Violate the California Administrative Procedure Act*, 52 CAL. W. L. REV. 1, 2 (2015) ("An 'underground regulation' includes any rule that meets the California APA's' broad definition of regulation but was not enacted according to the statute's procedures. Such regulations are categorically unenforceable.").

[10] Tonya Riley, *State Legislators Aren't Waiting for Congress to Regulate Children's Privacy*, CYBERSCOOP (Jan. 17, 2023), https://www.cyberscoop.com/california-age-appropriate-design-code-oregon-privacy/ [https://perma.cc/2Q7M-QBVH].

differences between both legal frameworks. Further, the Article considers the possible impact of the California Design Act in light of the Children's Online Privacy Protection Act of 1998 ("COPPA")—the federal pre-existing online child privacy framework.

Increasingly, children's traditional daily offline activities have turned into online activities and children more frequently access the internet, which increases opportunities for corporate surveillance and monetization of children's behaviors. Thus, in the modern era both children's online and traditional offline actions can be monitored and monetized. The California Design Act's incorporation of several of the U.K. Design Code's standards, such as privacy by design and default, data protection impact assessment obligations, and restrictions on monetization and tracking children without their knowledge may lead to improved privacy protections for children in some contexts. Additionally, both sources of law represent a departure from the existing approach of treating parents as the main gatekeepers of children's privacy given both frameworks' emphasis on corporate actors considering the best interests of children. This is perhaps an attempt to impose some aspect of a fiduciary duty on covered entities. This shift away from an overreliance on notice and choice to a focus on children's best interests may facilitate the development of online services that are better for children's privacy in some settings. The California Design Act's notable coverage of older children could also fill the regulatory gap left open by the limited under thirteen age range found in COPPA.

Despite the potential effectiveness of the California Design Act in some areas, the Article exposes underappreciated limitations in the Act's text, such as the seeming exclusion of Internet of Things ("IoT") devices. The Article also highlights notable challenges to the California Design Act's validity, such as First Amendment and federal preemption concerns, which may impede both the Act's legislative goals and successful transatlantic privacy law harmonization efforts. Additionally, many of the indicators used in the California Design Act to determine whether an entity is subject to the Act are similar to those found in COPPA's framework. Given these similarities, the California Design Act does not appear to be a significant departure from COPPA's framework in that regard.. It is also unclear whether the California Design Act's age estimation provisions and associated limits on the use of personal information collected for those purposes will lead to more data collection or alternatively, effectively address concerns about children's

anonymity. Thus, the California Design Act seemingly offers a mixed bag of privacy protections that in some instances could raise its own concerns.

Regardless of the outcome of the ongoing challenge to the California Design Act, the Article makes an enduring and valuable contribution to the privacy law field and existing debates on children's privacy by (1) exposing in detail the privacy concerns that children face in the IoT era from both child directed and general audience products and services, (2) highlighting the unique inescapable obstacles that U.S. legislators may face in their attempts to better protect children's online privacy, (3) providing an evaluation of the U.K. Design Code for a U.S. privacy law audience, and (4) proposing alternative legislative paths to more adequately safeguard children's privacy in the United States. Beyond its scholarly contribution, this Article is also of practical interest to companies, policymakers, privacy advocates, and individuals interested in better understanding the shifting child privacy landscape and potential compliance obligations. Indeed, on May 9, 2024, Maryland's governor signed into law the Maryland Age Appropriate Design Code Act, which is modeled in part after the California Design Act and is scheduled to become operative on October 1, 2024.[11] This highlights the importance and potential long-lasting influence of the California Design Act on U.S. privacy law.

The U.K. Design Code and the California Design Act both emerged in response to several alarming concerns about children's privacy, including the extent to which children are being *datafied* (the idea that their everyday actions can transform into data points through data collection by corporate actors). By focusing on the U.K. Design Code and the California Design Act, the Article seeks to shed light on how and to what extent the United States and the United Kingdom implement the ideal of protecting children's online privacy in the modern era. Indeed, corporate entities now collect

---

[11] *See* Allison Grande, *Maryland Enacts Data Privacy, Kids Digital Safety Laws*, LAW360 (May 9, 2024) https://www.law360.com/articles/1835510/maryland-enacts-data-privacy-kids-digital-safety-laws [https://perma.cc/FP2M-78TM] (reporting that the Maryland Age-Appropriate Design Code Act "is scheduled to take effect on Oct. 1, 2024 [and] is largely modeled after California's groundbreaking Age-Appropriate Design Code Act"); 2024 Bill Text MD S.B. 571. Although the Maryland Age-Appropriate Design Code Act is based in part on the California Design Act, there are important differences between both laws, such as the lack of an express age estimation requirement in the Maryland act. These differences are likely an attempt to avoid the current constitutional challenges plaguing the California Design Act.

unprecedented amounts of data about children in a vast array of contexts. Information about children's bodies, preferences, daily activities, and social interactions are increasingly becoming part of the digital sphere.[12] As the Federal Trade Commission ("FTC") has observed, "children and teens face greater risks of immediate and long-term dangers" from the modern-day expansion of surveillance services and products.[13]

Children more frequently access services and goods online via their smartphones, tablets, computers, and connected toys and other objects that make up the IoT. It is estimated that "one in three internet users is a child."[14] One study on children's use of modern technology found that 88% of children between the ages of thirteen and eighteen own a smartphone, 64% of those children own a desktop or laptop, and 36% of those children own a tablet.[15] This hyperconnectivity provides various opportunities for multiple companies to collect and potentially monetize detailed information about children.

One report estimates that "the average U.S. household now has a total of 25 connected devices."[16] The IoT has ushered in a new era in which numerous objects can connect to the internet. IoT devices are often continuously dependent on the corporate provision of software and services, such as mobile apps, for continued and optimal device functionality. This ongoing relationship between IoT firms and device users can enable persistent data collection and surveillance. IoT devices now include once ordinary non-connected

---

[12] *See* Donell Holloway, *Surveillance Capitalism and Children's Data: The Internet of Toys and Things for Children*, 170 MEDIA INT'L AUSTL. 27, 34 (2019).

[13] FED. TRADE COMM'N, FACT SHEET ON THE FTC'S COMMERCIAL SURVEILLANCE AND DATA SECURITY RULEMAKING, https://www.ftc.gov/system/files/ftc_gov/pdf/Commercial%20Surveillance%20and%20Data%20Security%20Rulemaking%20Fact%20Sheet_1.pdf [https://perma.cc/TYR2-SWZ4].

[14] DUNCAN MCCANN, NEW ECONOMICS FOUND., I-SPY: THE BILLION DOLLAR BUSINESS OF SURVEILLANCE ADVERTISING TO KIDS 2 (2021), https://neweconomics.org/uploads/files/i-Spy__NEF.pdf [https://perma.cc/D2UX-MAB7].

[15] *See* VICTORIA RIDEOUT ET AL., THE COMMON SENSE CENSUS: MEDIA USE BY TWEENS AND TEENS 22 (Jennifer Robb ed., 2022), https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf [https://perma.cc/7V35-M8H9].

[16] CHRIS ARKENBERG ET AL., HOW THE PANDEMIC HAS STRESS-TESTED THE CROWDED DIGITAL HOME 3 (Matthew Budman et al. eds., 2021), https://www2.deloitte.com/content/dam/insights/articles/6978_TMT-Connectivity-and-mobile-trends/DI_TMT-Connectivity-and-mobile-trends.pdf [https://perma.cc/Q3K6-PWTA].

household objects, such as televisions, refrigerators, washing machines, doorbells, coffee pots and relatively newer objects, such as smart speakers.

Increasingly, companies are flooding the consumer market with internet-connected toys. These toys can collect and learn information about a child's behaviors and activities and adjust operations accordingly.[17] Smart toys can also have geolocation and speech recognition capabilities as well as cameras and microphone features.[18] Even the U.S. Federal Bureau of Investigation acknowledged that IoT toys "could put the privacy and safety of children at risk due to the large amount of personal information that may be unwittingly disclosed."[19]

Even when devices are not directed specifically towards children, they can collect information about children. For instance, Amazon's general audience "Alexa-enabled smart speakers," can capture data about family members, including children's voices and their names.[20] Amazon's devices have captured children's apologies "to their parents after being disciplined" and recorded children as young as seven "asking Alexa questions about terms like 'pansexual.'"[21] Amazon also reportedly collected more than 90,000 Alexa recordings on one family since 2017, averaging about seventy a day.[22] While customers may have the ability to opt out of this type of continuous surveillance, doing so may negatively impact access to various services and features associated with the device.[23]

---

[17] *See* Public Service Announcement, Federal Bureau of Investigation, Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children (July 17, 2017), https://www.ic3.gov/Media/Y2017/PSA170717 [https://perma.cc/TWY2-98Z6].

[18] *See id.*

[19] *Id.*

[20] Chris Kirkham & Jeffrey Dastin, *A Look at the Intimate Details Amazon Knows About Us*, REUTERS (Nov. 19, 2021), https://www.reuters.com/technology/look-intimate-details-amazon-knows-about-us-2021-11-19/ [https://perma.cc/RR2Y-HC9B].

[21] *Id.*

[22] *See* Jeffrey Dastin et al., *Amazon Wages Secret War on Americans' Privacy, Documents Show*, REUTERS (Nov. 19, 2021), https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/#sidebar [https://perma.cc/8LWC-FCFK].

[23] *See Amazon Echo Dot Kids Edition*, MOZILLA (Nov. 8, 2021), https://foundation.mozilla.org/en/privacynotincluded/amazon-echo-dot-kids-edition/ [https://perma.cc/RN75-DEX9].

Amazon is already expanding its IoT offerings to include not only smart speakers, but also a "flying indoor surveillance" home drone, a surveillance robot with a built-in camera that can move from room to room, a smart screen to allow children to "make video calls," and a "15-inch wall mounted version of its Echo Show Screen" that will be able to observe users' in-home activities.[24] Amazon also plans to offer a new virtual assistant aimed at children that uses Disney characters in partnership with Disney.[25]

While the IoT potentially provides some benefits to businesses, parents, and children, such as convenience, efficiency, easier access to information and frictionless user experiences, the IoT also raises significant concerns about children's privacy. These concerns include widespread corporate surveillance that contributes to the datafication of children's in-home and public activities; possible reductions in children's ability to be anonymous and shield themselves while conducting ordinary activities, and the potential for IoT data, along with other sources of information, to be monetized and used to impact children's behaviors and influence the opportunities they receive. As more objects are replaced by their IoT equivalents and companies expand their IoT offerings, these potential privacy concerns deepen for children, especially given that they leave longer and more detailed digital footprints than past generations. Persistent surveillance and monetization of children's traditional online activities and IoT related activities can also generate concerns about the meaningfulness of consent to data practices and may pose civil liberty risks.

Given previous bipartisan support at the federal level for the adoption of a comprehensive federal privacy statute, Congress could consider adopting federal privacy legislation that takes a holistic approach to privacy and data security protection while simultaneously addressing the needs of children and adults.[26]

---

[24] Heather Kelly et al., *Amazon's Newest Products Expand Its Surveillance Inside the Home*, WASH. POST (Sept. 28, 2021), https://www.washingtonpost.com/technology/2021/09/28/amazon-event-echo-ring-launch/ [https://perma.cc/AKU5-9LLM].

[25] *See id.*

[26] *See* Allison Grande, *Data Privacy Bill Not Dead Yet, House Commerce Heads Say*, LAW360 (Sept. 29, 2022), https://www.law360.com/technology/articles/1533273/ [https://perma.cc/S67T-5CU8]. In fact, as this Article went to publication, some members of Congress have agreed on a deal for one such federal bill. *See* Allison Grande, *Key Congressional Leaders Float Sweeping Data Privacy Bill*, LAW360 (Apr. 8, 2024), https://www.law360.com/consumerprotection/articles/1822682 [https://perma.cc/4ZN3-2S9T]; American Privacy Rights Act, 118th Cong. (2024),

Federal privacy legislation could directly address privacy issues associated with the IoT, include specific restrictions on the trade of data or restrictions on the timing of consent like other sources of law, such as the Uniform Commercial Code ("UCC"), as well as impose privacy and security by design and default obligations, data minimization and data retention requirements. Congress could also consider calls for the imposition of fiduciary like duties.

The remainder of this Article proceeds as follows: Part I highlights two key data-driven practices that impact children and that are enabled by or flow from IoT devices and various other technological advancements, namely (i) persistent monitoring of children's online and traditional offline actions and the collection of numerous types of data, and (ii) various forms of data monetizations. I contend that these data-driven practices may contribute to concerns about decreasing levels of anonymity, and corporate exploitation of children's data. Additionally, these practices may raise civil liberty concerns. Consent and control may also be less meaningful in the IoT context. Further, weaknesses in companies' anonymization and aggregation techniques may not sufficiently address data-driven concerns. Part II conducts a detailed comparative analysis of the U.K. Design Code and the California Design Act and highlights relative similarities and notable differences between both frameworks while conducting a broader field of inquiry that offers potential reasons for the notable differences in both frameworks and assesses the ability of the California Design Act to remedy the concerns noted in Part I. This part also exposes potential limitations in, and challenges to the validity of, the California Design Act and highlights important similarities and differences between the California Design Act and COPPA, which may impact the reach and effectiveness of the California Design Act. Part III concludes by offering a path forward via the adoption of a baseline federal privacy statute.

---

https://www.commerce.senate.gov/services/files/3F5EEA76-5B18-4B40-ABD9-F2F681AA965F [https://perma.cc/9JK5-9JWS] [hereinafter APRA] (Although it is a Senate bill, no number has been assigned at the time of this writing, which is why the URL and a permalink have been provided).

I. DATA-DRIVEN PRACTICES

Increasingly, IoT devices and various other technological developments enable surveillance. Children's mundane offline activities, such as turning on a light, playing with a toy or ringing a neighbor's doorbell, are all transformed into online activities and are datafied via IoT devices and other systems that connect to the internet. These ordinary activities generate millions of data points that, once converted and collected, create both the possibility of corporate monetization and the ability to paint a detailed picture of children's behaviors and preferences, a picture that may even include how they grew up if collected over time. Similarly, there is the risk that other corporate entities, government officials, and other actors may access the data. This possibility may raise civil liberty concerns. Parental and child consent to corporate data practices may be less meaningful given the interconnected nature of IoT devices and services, which often rely on various entities to provide connected services. These various entities may have different privacy policies and data practices which parents and children may be unaware of or unable to understand. These variations may also contribute to parents and children having less control of their data. Additionally, by expanding children's online activities to include the performance of tasks and events that children historically performed offline without leaving a data trail, the IoT and other technological developments, such as facial recognition technology, may contribute to the ongoing erosion of children's ability to be anonymous. This offline-online datafication may reduce children's ability to shield their behaviors and personality traits from those who seek to commodify their experiences. Additionally, this section also highlights the limits of anonymization and aggregation in protecting children's privacy.

a. Datafication and Surveillance

Today's children are being surveilled while they are at school, home, and out in public. As a result, companies can collect a vast array of detailed information about children and their families and

observe many of their daily activities.[27] These data include video and audio recordings, location data, health-related data, and biometric-related data among other kinds. These data are often collected by IoT devices and toys and various other online services.

i. Audio, Video and Biometric Data

As more parents introduce IoT toys and devices into their homes, conversations and activities children could once engage in at home without immediate disclosure to anyone, let alone corporate entities, can now be more easily observed, monitored, and disclosed. Even when privacy-conscious parents elect to limit their families use of IoT surveillance devices, the prevalence of these devices in other homes may still lead to data collection. For example, Amazon's Ring cameras can capture videos and audio of visitors who have no contractual relationship with Amazon. While the identity of individuals captured in these recordings may not always be revealed, the frequency of the data collection is concerning and could lead to identification in the future, especially if combined with other data about an individual. Amazon is currently facing an ongoing lawsuit alleging that its Ring devices collected, without consent, the face templates of non-Ring device owners "who came into contact with" Ring devices in violation of Illinois' Biometric Information Privacy Act ("BIPA").[28]

---

[27] *See* GIRARD KELLY ET AL., STATE OF KIDS' PRIVACY 51, 54 (2021), https://www.commonsensemedia.org/sites/default/files/research/report/common-sense-2021-state-of-kids-privacy.pdf [https://perma.cc/94NU-26L9].

[28] *See* Wise v. Ring LLC, No. C20-1298-JCC, 2022 U.S. Dist. LEXIS 138399 (W.D. Wash. Aug. 3, 2022); Allison Grande, *Ring Can't Ditch Privacy Suit over Visitors' Face Scans*, LAW360 (Aug. 4, 2022, 10:15 PM), https://www.law360.com/articles/1518107 [https://perma.cc/G2X3-TJBM]. Several states and at least one municipality have adopted laws regulating the collection and use of biometric identifiers. *See, e.g.*, 740 ILL. COMP. STAT. ANN. 14/15 (2022); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2022); WASH. REV. CODE § 19.375.010 (2022); N.Y.C. ADMIN. CODE §§ 22-1201–22-1205 (2022); Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things,* 59 B.C. L. REV. 423, 488-96 (2018) [hereinafter Elvy, *Commodifying Consumer Data*]; Sophie L. Kletzien & Mark H. Francis, *NYC Passes Biometric Data Protection Laws Aimed at Businesses, Smart Access Building Owners*, HOLLAND & KNIGHT (Aug. 19, 2021), https://www.hklaw.com/en/insights/publications/2021/08/nyc-passes-biometric-data-protection-laws-aimed-at-businesses [https://perma.cc/3W45-JBU6]. There have been several legislative proposals to revise BIPA. *See, e.g.*, Charles N. Insler, *Will the Proposed Amendments to the Biometric Information Privacy Act (BIPA) Be Retroactive?*, BUS. L. TODAY (Apr. 30, 2021),

One frequently contested issue under statutes such as BIPA is whether data gleaned from audio recordings and videos qualifies as a biometric identifier.[29] If an IoT device captures a child's image or voice, a state's biometric data statute and its accompanying protections may not apply if the data collected does not qualify as a biometric identifier. However, pictures, videos, and audio recordings can turn into biometric identifiers, such as face prints, which can help identify individuals with the use of facial recognition technology.[30] Consider that, prior to dropping its facial recognition program, Meta could identify individuals in photos posted on its platform.[31]

IoT toys and other types of general audience IoT devices can also collect biometric identifiers. The Cozmo robot collects biometric identifiers by using facial recognition technology to scan children's faces and identify them and their pets.[32] The robot can also detect

---

https://businesslawtoday.org/2021/04/will-proposed-amendments-biometric-information-privacy-act-bipa-retroactive/ [https://perma.cc/TQ92-KUE8] (discussing the amendments proposed to BIPA by the Illinois state legislature).

[29] *See, e.g.*, Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 U.S. Dist. LEXIS 149604, at *13–14 (N.D. Ill. Sept. 15, 2017) (denying Shutterfly's motion to dismiss and reasoning that "advances in technology are what drove the Illinois legislature to enact the [Illinois statute] in the first place, so it is unlikely that the statute sought to limit the definition of biometric identifier by limiting how the measurements are taken"); *Rivera v. Google, Inc.*, 238 F. Supp. 3d 1088, 1095, 1104 (N.D. Ill. 2017) (denying Google's motion to dismiss); Gullen v. Facebook.com, Inc., No. 15 C 7681, 2016 U.S. Dist. LEXIS 6958, at *9 (N.D. Ill. Jan. 21, 2016) (dismissing plaintiff's claim); Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015) (denying defendant's motion to dismiss and reasoning given statutory definitions plaintiff "plausibly stated a claim" by alleging that "defendants are using his personal face pattern to recognize and identify [him] in photographs posted to Websites."); *see also* Elvy, *Commodifying Consumer Data*, *supra* note 28, at 490 n.344 (discussing these cases).

[30] *See Biometrics*, PRIV. INT'L, https://privacyinternational.org/learn/biometrics (last visited Oct. 14, 2022) [https://perma.cc/7F4Q-XQJP]; Jeff John Roberts, *Judge Says Customers Can Sue over Face Scans*, FORTUNE (Sept. 19, 2017, 4:21 PM), https://fortune.com/2017/09/19/shutterfly-face-scan/ [https://perma.cc/UV6P-M2ZK]; James Vincent, *Lyrebird Claims It Can Recreate any Voice Using Just One Minute of Sample Audio*, VERGE (Apr. 24, 2017), https://www.theverge.com/2017/4/24/15406882/ai-voice-synthesis-copy-human-speech-lyrebird [https://perma.cc/PM7B-BEWJ] (discussing a similar technology).

[31] *See* Kashmir Hill & Ryan Mac, *Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System*, N.Y. TIMES (Nov. 5, 2021), https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html [https://perma.cc/PUX7-UDTS].

[32] *See* DIGITAL DREAM LABS, LLC., COZMO 2.0 EDUCATIONAL TOY ROBOT, https://www.digitaldreamlabs.com/products/cozmo-robot

when children are smiling.[33] Amazon's Astro robot uses biometric scans in its facial recognition function and collects data about how device owners and members of their household move around their homes.[34]

Some homebuilders, are already integrating IoT devices into newly constructed homes; in fact, one industry survey estimates that "32% of new homes" have IoT doorbell cameras.[35] In 2020, sales of IoT doorbells in the United States reached approximately 7.9 million.[36] IoT cameras and doorbells, which often can function both inside and outside of homes, are so ubiquitous that an analysis of their use in Washington, D.C. determined that, on a walking path of less than one mile between a public charter school and its soccer field, sixth to twelfth grade students had to walk by approximately thirteen Ring cameras if they chose the shortest route.[37] The owners of these Ring cameras often shared their Ring footage on social media.[38] The investigation found that approximately 4,000 video footage posts on the Neighbors app associated with Ring devices

---

[https://perma.cc/C2QF-BL5W] (last visited Oct. 15, 2022) [hereinafter COZMO 2.0]; Emma Day, *Children's Connected Toys: Part 1*, MEDIUM (Sept. 14, 2021), https://medium.com/@emmadaylaw/childrens-connected-toys-part-1-b231df9c6e82 [https://perma.cc/7GP7-66LU] (noting that the "app that invites the child to 'get to know Cozmo better' by having the robot scan the child's face").

33 *See* COZMO 2.0, *supra* note 32 ("[T]he new 2MP camera will enhance Cozmo's facial recognition; improving his ability to recognize pets and even know if you are smiling.")

34 *See* Laura Hautala, *Amazon Astro Is the Cute Face That Makes Tech Feel Like a Friend*, CNET (Apr. 22, 2022), https://www.cnet.com/home/smart-home/amazon-astro-is-the-cute-face-that-could-make-you-treat-tech-like-your-friend/ [https://perma.cc/ZB5X-9DMS]; Samantha Murphy Kelly, *Amazon Is Always Watching*, CNN BUS. (Oct. 3, 2022, 3:17 PM), https://www.cnn.com/2022/10/02/tech/amazon-product-event/index.html [https://perma.cc/64DD-RBHR].

35 AIHA NGUYEN & EVE ZELICKSON, AT THE DIGITAL DOORSTEP: HOW CUSTOMERS USE DOORBELL CAMERAS TO MANAGE DELIVERY WORKERS 17 (2022), https://datasociety.net/wp-content/uploads/2022/10/AttheDigitalDoorstepFINAL.pdf [https://perma.cc/F9UL-3KD7].

36 *See id.*

37 *See* Dell Cameron & Dhruv Mehrotra, *Ring's Hidden Data Let Us Map Amazon's Sprawling Home Surveillance Network*, GIZMODO (Dec. 9, 2019), https://gizmodo.com/ring-s-hidden-data-let-us-map-amazons-sprawling-home-su-1840312279 [https://perma.cc/FY2S-6SSK]; *see also* Matthew Guariglia & Dave Maass, *LAPD Requested Ring Footage of Black Lives Matter Protests*, ELEC. FRONTIER FOUND. (Feb. 16, 2021), https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests [https://perma.cc/6CBP-BQZY].

38 *See* Guariglia & Maass, *supra* note 37; Cameron & Mehrotra, *supra* note 37.

referenced children and, although the app did not disclose the physical addresses of Ring owners and app users, the app disclosed, with each post, geographic coordinates, such as "latitude and longitude[,] with up to six decimal points of precision, accurate enough to pinpoint roughly a square inch of ground."[39]

ii. Health-Related Data and Location Data[40]

In addition to the other types of data mentioned earlier, companies can also collect health-related data from children via wearable IoT devices and mobile apps. The health monitors and fitness device market was expected to grow "to $41.8 billion in 2023."[41] Consider that Weight Watchers' diet mobile app reportedly collected data on children younger than thirteen years old.[42] Weight Watchers allegedly encouraged children to falsely indicate that they were over the age of thirteen to avoid obtaining parental consent as

---

[39] Cameron & Mehrotra, *supra* note 37.

[40] I generally use the term "health-related data" to refer to data relating to an individual's health that is collected by IoT devices, mobile apps and other services, excluding health care data, medical records data and other types of data collected in a clinical setting. Health-related data collected by businesses via IoT devices and services can be viewed as distinct from health care or medical records data obtained during treatment from a health care provider considering the circumstances under which the data are collected even though similar data could be collected or IoT devices used in both settings. Admittedly, companies may combine health related-data with other sources of information such that health-related data may not be standalone data. If legislators attempt to impose specific restrictions for health-related data, legislators would need to provide guidance on which types of data would be subject to any such specific restrictions.

[41] Michael Essery, *Mobile Health Devices Market to Grow 8-Fold to $41.8 Billion in 2023*, LUX RSCH. (July 1, 2014), http://www.luxresearchinc.com/news-and-events/press-releases/read/mobile-health-devices-market-grow-8-fold-41sag8-billion-2023 [https://perma.cc/5GDF-U9X9].

[42] *See* Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief at 11, U.S. v. Kurbo, Inc., No. 22-CV-946 (N.D. Cal. Feb. 16, 2022) ("[D]efendants collected personal information including names, email addresses, and persistent identifiers, as well as other information like height, weight, food intake, and activity"); Kate Gibson, *Weight Watchers Diet App Collected Data on Kids as Young as 8, FTC Says*, CBS NEWS (Mar. 4, 2022), https://www.cbsnews.com/news/weight-watchers-diet-kids-ftc/ [https://perma.cc/KP56-ER3A]; Corinne Reichert, *FTC Takes Action Against WW for Collecting Children's Health Data*, CNET (Mar. 4, 2022), https://www.cnet.com/news/privacy/ftc-takes-action-against-ww-for-collecting-childrens-health-data/ [https://perma.cc/C52W-QAHQ].

required by COPPA.[43] The FTC ultimately required the company to delete the data as well as the "algorithms derived from the data"—a nascent evolving FTC remedy, described by some as algorithmic destruction or disgorgement.[44]

Another company, Neebo, manufactures a wearable IoT wristband that parents of newborns can control through a mobile app to monitor newborns' heart rates, oxygen levels, and thermal state.[45] Similarly, toy giant Mattel previously offered its own wearable ankle IoT device to monitor babies' sleep patterns, temperature, and heart rate.[46] Owlet, by comparison, offers an IoT baby monitor camera and wearable IoT infant sock that uses predictive sleep technology and tracks blood oxygen and heart rate levels.[47]

---

[43] *See* Gibson, *supra* note 42; 16 C.F.R. 312.5.

[44] Press Release, Fed. Trade Comm'n, FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data (Mar. 4, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive [https://perma.cc/5Q5A-N7S7]; *see also* Rebecca Kelly Slaughter, *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*, 23 YALE J. L. & TECH 1, 39 (2021).

[45] *See* NEEBO, https://neebomonitor.com [https://perma.cc/2DRQ-ST2T] (last visited Oct. 15, 2022).

[46] *See* Aditi Pai, *Mattel Acquires Baby Health Wearable Maker Sproutling*, MOBI HEALTH NEWS (Feb. 1, 2016), https://www.mobihealthnews.com/content/mattel-acquires-baby-health-wearable-maker-sproutling [https://perma.cc/S3FS-XWRM].

[47] *See* OWLET, https://www.owletcare.com/ [https://perma.cc/V38X-XC57] (last visited Oct. 15, 2022). The Food and Drug Administration ("FDA") has attempted to regulate the claims of some IoT baby devices under the Federal Food, Drug and Cosmetic Act. In 2021, for instance, the FDA issued a warning letter to Owlet, regarding claims made by the company about monitoring blood oxygen and pulse rate levels. These claims, according to the FDA, brought the device within the definition of a medical device "intended for use in the diagnosis of disease or other conditions," which requires marketing authorization from the FDA. *See* Warning Letter from Malvina Eydelman, Director, Ctr. Devices & Radiological Health, to Kurt Workman, CEO, Owlet Baby Care, Inc. (Oct. 5, 2021). In addition to potential FDA supervision, there are various state laws that can impact children's health-related data. As one scholar noted, "state [health data] laws are varied and inconsistent, often providing piecemeal protection for some types of data but not others and these protections may be scattered among multiple laws." SHARONA HOFFMAN, ELECTRONIC HEALTH RECORDS AND MEDICAL BIG DATA: LAW AND POLICY 135 (Cambridge Univ. Press 2016) (alteration in original). While the federal Health Insurance Portability and Accountability Act ("HIPAA") does not apply to a large segment of the health-related data IoT devices collect because IoT companies often do not qualify as HIPAA covered entities, state privacy laws can, in some instances, cover children's health-related data even when such data is not subject to HIPAA. *See* 42 U.S.C. §§ 1320d–1320d-8 (2012) (statutory authority); 45 C.F.R. § 160.103 (2022) (defining a "covered entity" as a "health plan," "health care clearinghouse,"

IoT smartwatches worn by children can also collect health-related data and real-time data about their location; they can even monitor their actions.[48] Location data can reveal intimate details about a child's life, including travel patterns, frequently visited locations, and daily activities. Location data could also be used to deduce children's preferences. As with other types of data, location data can be combined with other sources of data, such as data obtained from cross-device tracking and data brokers, to paint a detailed picture of an individual's life. Cross-device tracking—connecting the activities of users "across [their] smartphones, tablets, desktop computers," and IoT devices—allows companies to obtain detailed information about device users.[49] Both the initial provider of the product or service and third-party firms can engage in this tracking.[50] In short, IoT devices and mobile apps and systems can enable frequent surveillance and the collection of various types of data about children in a dazzling array of contexts.

iii. Civil Liberty Concerns

Once collected data about children can potentially be disclosed to governmental authorities. Amazon has disclosed to law enforcement footage captured by users' Ring cameras in accordance

---

"health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter," or "business associate of another covered entity"); 45 C.F.R. §§ 160.101–.534 (privacy rule); 45 C.F.R. §§ 164.302–.318 (security rule); Elvy, *Commodifying Consumer Data*, *supra* note 28, at 496-500; Tawanna Lee & Antonio Reynolds, *All Data Is Not HIPPA Data – Healthcare Covered Entities Should Pay Close Attention to State Privacy Laws Regulating the Health IoT Ecosystem*, JD SUPRA (July 13, 2021), https://www.jdsupra.com/legalnews/all-data-is-not-hipaa-data-healthcare-3523068/ [https://perma.cc/5PRX-822V] ("State privacy laws are currently the main source of regulation for healthcare adjacent data, and apply much more broadly than HIPAA (*e.g.*, most state privacy laws are not limited to Covered Entities).").

[48] *See* Lee Mathews, *Your Child's GPS Watch Could Be Exposing Their Location in Real-Time*, FORBES (Feb. 5, 2019), https://www.forbes.com/sites/leemathews/2019/02/05/your-childs-gps-watch-could-be-exposing-their-location-in-real-time/?sh=e0f5b3226452 [https://perma.cc/2PHQ-WHXC].

[49] *See* FED. TRADE COMM'N, CROSS-DEVICE TRACKING 1-10 (2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf [https://perma.cc/EF7V-JSQU] [hereinafter FTC CROSS-DEVICE REPORT] (alteration in original).

[50] *See id.* at 3-4, 8.

with its policy that permits disclosures with user consent or in accordance with warrants or "emergency circumstances."[51] Local police departments previously asked for videos of Black Lives Matter protesters captured by Ring cameras,[52] and children have also participated in such protests.[53] Such policies raise potential civil liberties issues. Individuals may become reluctant to engage in political activity for fear of government surveillance. As Christopher Slobogin argues, "[a]nonymity in public promotes freedom of action and an open society," and a "[l]ack of public anonymity promotes conformity and an oppressive society."[54]

The prevalence of IoT objects may condition children at an early age to accept continuous surveillance.[55] Increasingly, children are unable to conduct daily activities without having their data collected. This growing data collection will likely decrease children's anonymity. After all, the more data points that are available about any given individual, the higher the chance of identification. Additionally, even if a child's identity is not revealed, surveillance and data collection can unmask their feelings, moods and desires, which effectively reduces their anonymity and, more generally, their ability to shield themselves and their reactions from others. The disclosure of such data by corporate actors to law enforcement officials may also make children more reluctant to participate in certain political activities as they grow older, which could have a disproportionate impact on members of historically marginalized groups. When children know that they are being subjected to surveillance, they may be "less likely to question authority or engage in critical thinking."[56] One study evaluating

---

[51] Guardian Staff and Agency, *Amazon Gave Ring Doorbell Videos to US Police 11 Times Without Permission*, GUARDIAN (July 13, 2022), https://www.theguardian.com/technology/2022/jul/13/amazon-ring-doorbell-videos-police-11-times-without-permission [https://perma.cc/YPP2-QEBH].

[52] Guariglia & Maass, *supra* note 37.

[53] *See* REBECCA DUBE, *Children Protest for Black Lives Matter*, TODAY (May 25, 2022), https://www.today.com/parents/11-powerful-photos-children-black-lives-matter-protests-t184119 [https://perma.cc/QU9W-RV3W].

[54] Christopher Slobogin, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 92 (Univ. Chicago Press 2007).

[55] *See* STACY-ANN ELVY, A COMMERCIAL LAW OF PRIVACY AND SECURITY FOR THE INTERNET OF THINGS 25-59, 269-310 (Cambridge Univ. Press 2021) [hereinafter ELVY, A COMMERCIAL LAW OF PRIVACY].

[56] KATIE JOSEFF, BEHAVIORAL ADVERTISING HARMS: KIDS AND TEENS, A GUIDE FOR POLICYMAKERS AND PARENTS FROM COMMON SENSE (2022), https://www.commonsensemedia.org/sites/default/files/featured-

families' use of IoT smart speakers found that some children expressed concerns about future data disclosures to others.[57]

iv. Meaningless Consent and Control

Under the notice and choice model which permeates U.S. privacy law, companies must generally obtain consent to collect and monetize data after disclosing their privacy practices. Depending on the age of the child, a firm may give parents or the child the option to opt-out or opt-in to data collection, surveillance, and data disclosures. However, multiple companies may have access to a child's data from the use of a single service or IoT product, which may make users' decisions authorizing data collection and surveillance less meaningful. Like other consumers, parents and children may not understand the legalese contained in privacy policies or the implications of consenting to corporate data practices.

Consider that Amazon's Echo Dot Kids device can be accompanied by various "Alexa Skills," which are apps mostly developed by third-party companies that can interact with Alexa.[58] By one estimate, there are more than 100,000 available Alexa Skills.[59] However, Amazon's privacy policy does not appear to govern any of the apps; instead, it is likely the privacy policy of the third-party that built the app that governs.[60] Research on these third-party companies found that 23.3% of studied companies' privacy policies did not adequately disclose corporate data practices and a

---

content/files/behavioral_-surveillance-advertising-brief.pdf [https://perma.cc/GEJ5-2CA8].

57 *See* Radhika Garg & Subhasree Sengupta, *"He Is Just Like Me": A Study of the Long-Term Use of Smart Speakers by Parents and Children*, 4 PROC. ACM ON INTERACTIVE, MOBILE, WEARABLE & UBIQUITOUS TECHS. 1, 1-24 (2020).

58 *Amazon Echo Dot Kids Edition*, *supra* note 23.

59 *See id*.

60 *See id*. ("When using Amazon Skills, be mindful that they are not operating under Amazon's privacy policy."); James Vincent, *Here's Why It's Important to Audit Your Amazon Alexa Skills (And How To Do It)*, VERGE (Mar. 5, 2021), https://www.theverge.com/2021/3/5/22315211/amazon-alexa-skills-how-to-remove-security-privacy-problems [https://perma.cc/EU6K-FGD5] ("Privacy policies are supposed to inform users about how their data is being collected and used, but Amazon doesn't require skills to have accompanying policies. Researchers found that only 28.5[%] of [U.S.] skills have valid privacy policies, and this figure is even lower for skills aimed at children—just 13.6[%].").

significant number of apps aimed at children did not have a privacy policy.[61]

The interconnected nature of IoT devices and services combined with the various providers associated with device functionality may also result in parents and children having less control of the data their IoT devices collect. For instance, deleting children's data from an Amazon device may not necessarily lead to full data deletion, even as it relates to transcripts of recordings obtained by a third-party company behind an Alexa Skills app.[62] It is also notable that the FTC has pursued Amazon for COPPA violations flowing from the indefinite storage of children's voices collected through Alexa and the Echo Dot speaker and improper notice.[63]

b. Data Monetization

Despite existing legal frameworks regulating parents' and children's data, companies frequently monetize these data. To some extent, this tendency likely exists because U.S. privacy frameworks often over-rely on the notice and choice model and privacy self-management.[64] As Daniel Solove observes, U.S. privacy law uses consent to "legitimize[] nearly any form of collection, use, or

---

[61] *See Amazon Echo Dot Kids Edition*, *supra* note 23; Anupam Das & Matt Shipman, *Study Reveals Extent of Privacy Vulnerabilities with Amazon's Alexa*, NC STATE: NEWS (Mar. 4, 2021), https://news.ncsu.edu/2021/03/alexa-skill-vulnerabilities/ [https://perma.cc/C39Q-Z3QF]; Christopher Lentzsch et al., *Hey Alexa, Is This Skill Safe?: Taking a Closer Look at the Alexa Skill Ecosystem* 4 (Nat'l Sci. Found., Grant No. CNS-1849997, 2021) ("[O]nly 24.2% of skills have a link to a privacy policy").

[62] *See Amazon Echo Dot Kids Edition*, *supra* note 23.

[63] *See* Complaint for Permanent Injunction, Civil Penalties, and Other Relief at 14, *Amazon.com*, No. 2:23-cv-00811 ("Amazon is an 'operator' subject to the [COPPA] Rule. Amazon operates the online services Echo Dot Kids Edition with FreeTime on Alexa and FreeTime Unlimited, both of which are directed to children under [thirteen]. Through the Echo Dot Kids Edition with FreeTime on Alexa and/or FreeTime Unlimited, Amazon collects personal information as defined in the COPPA Rule from children under [thirteen], including voice recordings and transcripts concerning the child combined with a persistent identifier.") (alteration in original); Ben Kochman, *Amazon to Pay $30M to End FTC's Alexa, Ring Privacy Claims*, LAW360 (May 31, 2023), https://www.law360.com/cybersecurity-privacy/articles/1683340 [https://perma.cc/2N9G-RC8C].

[64] *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV. 1879, 1880 (2013) (defining privacy-self management as the primary approach in privacy law in which "the law provides people with a set of rights to enable them to make decisions about how to manage their data").

disclosure of personal data."[65] Firms can monetize the data collected about children's online activities in various ways, including selling the data to third parties, using the data for adverting purposes and internal monetizations.[66]

i. Child Data Sales

Companies can sell data about individuals to third-party entities.[67] Children are not immune from this type of monetization. A 2020 policy statement by the American Academy of Pediatrics notes that, in the online context, "[u]ser data can be aggregated and stored, sold to third parties, and used to infer personal characteristics, such as sexual orientation or health problems."[68]

In 2021, Life360, a mobile app "used by 33 million people worldwide" which allows parents to monitor children's location, allegedly sold non-anonymized and non-aggregated precise location data, including children's data, to multiple data brokers.[69] The company's privacy policy indicates that it sells data obtained from families' use of its app.[70] Not surprisingly, a study evaluating

---

[65] *Id.*

[66] *See* Jeff Graham, *Our State of Kids' Privacy Research Indicates the Selling of Data Is About to Completely* Change, COMMON SENSE EDUC. (Mar. 29, 2022), https://www.commonsense.org/education/articles/a-majority-of-apps-are-about-to-come-clean-and-say-theyve-been-selling-your-data-all-along [https://perma.cc/W55J-ZTB3].

[67] *See id.*; Staff, *Your Data Is Shared and Sold . . . What's Being Done About It?*, KNOWLEDGE AT WHARTON (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ [https://perma.cc/WJR2-7M37].

[68] Jenny Radesky et al., *Digital Advertising to Children*, 146 AM. ACAD. PEDIATRICS 1, 2 (2020).

[69] Jon Keegan & Alfred Ng, *The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users*, MARKUP (Dec. 6, 2021), https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user [https://perma.cc/YN2Q-9G2M]; *see* David Priest, *Life360 App Is Selling Data from Millions of Families, Report Says*, CNET (Dec. 8, 2021), https://www.cnet.com/home/security/life360-app-is-selling-data-from-millions-of-families-report-says/ [https://perma.cc/PE2D-ZXYD]. The company subsequently reported that it would no longer sell precise location data, but left the door open to the sale of anonymized data. Jon Keegan & Alfred Ng, *Life360 Says It Will Stop Selling Precise Location Data*, MARKUP, (Jan. 27, 2022, 5:30 PM), https://themarkup.org/privacy/2022/01/27/life360-says-it-will-stop-selling-precise-location-data [https://perma.cc/SLH8-ZLBC].

[70] *See* Keegan & Ng, *supra* note 69.

the privacy practices of companies offering online children's products and services found that, since 2020, there was "an approximate increase of 56%, from 9% to 14%, of products that disclose that they sell data."[71]

Children's data can also be sold and transferred in bankruptcy proceedings. Privacy policies often authorize the disclosure of consumer data in the event of a change in companies' structure. Consider that children's data was part of Filip Technology Inc.'s assets when the company filed for bankruptcy.[72] Prior to bankruptcy, the company sold wearable IoT devices to parents for children's use.[73] Additionally, children's data can be disclosed and sold if an IoT company merges or is acquired by a third-party company.

ii. Internal Monetizations and Behavioral Advertising

Even when the companies that initially collect children's data do not sell or share the data, but instead retain the data internally, the data can still be combined into datasets upon which queries are run to reveal other insights about individuals. These insights not only can further marketing efforts, but they can also help to construct, enhance, and train firms' algorithmic systems,[74] which may have intellectual property protections.[75] Data used to train algorithmic decision making systems can "reflect historical and enduring patterns of prejudice" and reinforce existing inequalities.[76]

---

71 KELLY ET AL., *supra* note 27, at 10.

72 *See* Elvy, *Commodifying Consumer Data*, *supra* note 28, at 430-31.

73 *See id.* at 430.

74 *See* Kate Kaye, *The FTC'S New Enforcement Weapon Spells Death for Algorithms*, PROTOCOL (Mar. 14, 2022), https://www.protocol.com/policy/ftc-algorithm-destroy-data-privacy [https://perma.cc/QG2P-Y2NJ] ("When it comes to today's data-centric business models, algorithmic systems and the data used to build and train them are intellectual property, products that are core to how many companies operate and generate revenue."); Staff, *supra* note 67 (discussing what data companies collect and the benefits to their algorithms that it brings); Slaughter, *supra* note 44, at 7-10 (discussing the concerns related to discrimination, which, in one instance, resulted "from the fact that the resumes used to train Amazon's algorithm reflected the male").

75 *See* Kaye, *supra* note 74; Megan J. Ryan, *Secret Algorithms, IP Rights, and the Public Interest*, 21 NEV. L.J. 61, 108 (2019) (noting that algorithms may be subject to trade secret protection).

76 Slaughter, *supra* note 44, at 7-8; *see* Avi Asher-Schapiro, *Global Exam Grading Algorithm Under Fire for Suspected Bias*, REUTERS (July 21, 2020, 8:41 AM),

Moreover, these systems can also enable discrimination by targeting individuals with neutral traits that serve as a proxy for a legally protected category, such as race or gender.[77] Additionally, inaccurate conclusions could be drawn about individuals using these systems.[78] For instance, facial recognition algorithms are prone to misidentifying minorities.[79]

Consider that retailers can use facial recognition and detection technologies and associated connected devices to reduce incidences of shoplifting as well to increase their profits by identifying, monitoring, and categorizing shoppers based on their shopping habits, age, gender, and race.[80] Facial detection technology can allow

---

https://www.reuters.com/article/us-global-tech-education-analysis-trfn/global-exam-grading-algorithm-under-fire-for-suspected-bias-idUSKCN24M29L [https://perma.cc/3263-MJNA] (As one international student describes, "I come from a low-income family—and my entire last two years [of high school] were driven by the goal of getting as many college credits as I could to save money on school" and "[w]hen I saw those scores," created from a statistical model rather than traditional final exams, "my heart sank") (alteration in original).

77 *See* Slaughter, *supra* note 44, at 20; Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1428 (2017) (discussing proxy discrimination in the personal data economy context).

78 *See* Slaughter, *supra* note 44, at 10-13.

79 *See* Elizabeth A. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STAN. TECH. L. REV. 1, 27 (2020) ("Some research indicates that facial recognition algorithms may not be as accurate at reading the faces of certain demographics, in particular African Americans."); Chad Boutin, *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NAT'L INST. STANDARDS & TECH. (Dec. 19 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software [https://perma.cc/T5N6-6YEB] (discussing a NIST study on facial recognition algorithms and noting that the NIST "the team saw higher rates of false positives for Asian and African American faces relative to images of Caucasians").

80 *See* Casey Aonso, *Malls Across Canada Are Using Facial Recognition Technology to Track Shoppers and It Sounds Like an Episode of Black Mirror*, NARCITY MEDIA GRP. (Nov. 3, 2018), https://www.narcity.com/malls-across-canada-are-using-facial-recognition-technology-to-track-shoppers-and-it-sounds-like-an-episode-of-black-mirror [https://perma.cc/NM5R-2GGN]; Eden Gillespie, *Are You Being Scanned? How Facial Recognition Technology Follows You, Even as You Shop*, GUARDIAN (Feb. 23, 2019), https://www.theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop [https://perma.cc/R2GZ-HW4U]; Rebecca Heilweil, *From Macy's to Albertsons, Facial Recognition Is Already Everywhere*, VOX MEDIA (July 19, 2021), https://www.vox.com/2021/7/15/22577876/macys-fight-for-the-future-facial-recognition-artificial-intelligence-storess-and-it-sounds-like-an-episode-of-black-mirror [https://perma.cc/6YPV-49PW]; Sergio Mannino, *How Facial Recognition Will Change Retail*, FORBES (May 8, 2020), https://www.forbes.com/sites/forbesbusinesscouncil/2020/05/08/how-facial-recognition-will-change-retail/?sh=6ee61a4c3daa [https://perma.cc/XPU2-B4VY]; Sarah Rieger, *At Least Two Malls Are Using Facial Recognition Technology to*

retailers to provide customized prices to specific consumers, while also capturing adults' and children's moods and facial responses to advertisements and in-store products in real time.[81] Once collected, retailers can send personalized deals to their customers via text message and emails and sell to advertisers the ability to provide "tailored advertisements within seconds."[82]

Some advocates of facial detection technology argue that they do not identify individuals but instead use this technology to determine peoples' characteristics.[83] As mentioned earlier, even if a child's identity is not revealed, the child's feelings and personal and emotional attributes could be inferred or unmasked and used for behavioral advertising. At a young age, children could lose the ability to shield their emotions and reactions from corporate actors who seek to monetize their responses. Additionally, a child's facial expression or response may not always accurately and consistently convey the child's emotions.[84] Firms could treat children and their parents differently "based on the possibly unreliable and inaccurate emotions these technologies detect and assign to" them.[85]

Consider that a study of mobile apps used by three, four and five year-old children found that 67% of studied apps collected digital identifiers and then shared that data to unrelated marketing entities.[86] It is estimated that 90% of educational tools used by students were designed, in part, to send data collected "to ad-technology companies, which could use it to estimate students'

Track Shoppers' Ages and Genders Without Telling, CBC (July 27, 2018), www.cbc.ca/news/canada/calgary/calgary-malls-1.4760964 [https://perma.cc/Z84G-MVW2]; Ben Sobel, *Facial Recognition Technology Is Everywhere. It May Not Be Legal.*, WASH. POST (June 11, 2015), www.washingtonpost.com/news/the-switch/wp/2015/06/11/facial-recognition-technology-is-everywhere-it-may-not-be-legal/?utm_term=.990800971bec [https://perma.cc/SKJ3-H35R]; Hannah Towey, *The Retail Stores You Probably Shop at That Use Facial-Recognition Technology*, BUS. INSIDER (July 19, 2021), https://www.businessinsider.com/retail-stores-that-use-facial-recognition-technology-macys-2021-7 [https://perma.cc/KMF2-DX24].

81 *See* Lindsey Barrett, *Ban Facial Recognition Technologies for Children – and for Everyone Else*, 26 B.U. J. SCI. & TECH. L. 223, 237 (2020); Gillespie, *supra* note 80; Mannino, *supra* note 80; Sobel, *supra* note 80.

82 Gillespie, *supra* note 80.

83 *See id*.

84 *See* Douglas Heaven, *Expression of Doubt*, 578 NATURE 502, 502-04 (2020).

85 ELVY, A COMMERCIAL LAW OF PRIVACY, *supra* note 55, at 46.

86 *See* Fangwei Zhao et al., *Data Collection Practices of Mobile Applications Played by Preschool-Aged Children*, 174 JAMA PEDIATRICS 1, 2, 4 (2020).

interests and predict what they might want to buy."[87] One study of child-directed mobile applications found approximately 12,000 mobile apps that have access to children's personal information did not have a privacy policy and that personal information, such as geolocation data, video and audio files, are "42% more likely to be shared with advertisers on child-directed mobile apps."[88]

A 2021 report by Common Sense Media, a non-profit organization, evaluating over 200 online products and services children use found that, while some companies that provide products intended for children indicate that they do not sell children's data to third parties, 49% of those businesses "still engage in additional monetization practices," such as third-party tracking and ad profiles.[89] According to one of the study's authors, one interpretation of the findings is that, at most, only 27% of studied companies do not sell children's data.[90] The report suggests that "companies are disclosing their data monetization practices in a manner that is inconsistent with the guidelines and clarifications" in the 2020 amendments to the California Consumer Privacy Act of 2018 ("CCPA"). [91] TikTok also reportedly sold to advertisers the data of eighty-nine million users, including minors as young as six..[92]

---

[87] Drew Harwell, *Remote Learning Apps Shared Children's Data at a "Dizzying Scale"*, WASH. POST (May 24, 2022), https://www.washingtonpost.com/technology/2022/05/24/remote-school-app-tracking-privacy/ [https://perma.cc/T9WA-7AK7]; *see also* Hye Jung Han, *"How Dare They Peep into My Private Life?": Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic*, HUM. RTS. WATCH (May 25, 2022), https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments? [https://perma.cc/H237-XUA9] ("Human Rights Watch found that children's educational websites installed as many third-party trackers on personal devices as do the world's most popular websites aimed at adults. Out of a total 124 EdTech websites, 112 websites (90[%]) placed third-party ad trackers on devices and browsers used by children.").

[88] PIXALATE, MOBILE APPS: GOOGLE VS. APPLE COPPA SCORECARD (CHILDREN'S PRIVACY) Q.1 2022 3 (2022), https://www.pixalate.com/hubfs/Reports_and_Documents/ [https://perma.cc/NVV8-NUAU] (due to unwieldy URL, only root URL is provided here, so please refer to permalink shown here for full, convenient access to this report).

[89] KELLY ET AL., *supra* note 27, at 51.

[90] *See* Graham, *supra* note 66 ("[A] more accurate interpretation would be that only 27% don't sell your data.").

[91] *Id.*

[92] *See* Bobby Allyn, *TikTok to Pay $92 Million to Settle Class-Action Suit over "Theft" of Personal Data*, NPR (Feb. 25, 2021),

With respect to ad profiles, children's data can also be shared with third-party companies via companies' real-time bidding and digital auction processes. Such processes allow companies to monetize individuals' data quickly and efficiently.[93] Once an individual visits a page, a bidding process begins involving multiple advertisers who simultaneously receive data about individuals, such as IP address, demographics, location, device information, possible interests, and potentially information on an individual's race, health status, and religion.[94]

Ad-tech companies then use these data to determine the price they are willing to pay to show their advertisement to the individual visiting the website. Even if an advertiser does not win the bid for the advertisement, they still can obtain data about the website visitor.[95] This process may arguably not be considered a traditional sale of data because, rather than paying for the data, the advertisers pay for the ability to show the advertisement on the page the individual visited, though it appears that they still can obtain information about the individual during the bidding process.[96] Thus, even if platforms contend that they do not sell individuals' data, allowing advertisers to target users with certain characteristics arguably reveals the personal data of these consumers.[97] This method of advertising could allow advertisers to view "metrics on which ad the user clicked on" and the category the user is associated with.[98] As data scientist Michal Kosinski argues, companies could use data obtained from targeted advertising and other sources of

---

https://www.npr.org/2021/02/25/971460327/tiktok-to-pay-92-million-to-settle-class-action-suit-over-theft-of-personal-data [https://perma.cc/6LF2-7ZGT].

93 *See* Alfred Ng, *What Does It Actually Mean When a Company Says, "We Do Not Sell Your Data"?*, MARKUP (Sept. 12, 2021), https://themarkup.org/the-breakdown/2021/09/02/what-does-it-actually-mean-when-a-company-says-we-do-not-sell-your-data [https://perma.cc/B8VY-UPYD].

94 *See id.*; *In re* Google RTB Consumer Priv. Litig., 606 F. Supp. 3d 935, 5-6 (N.D. Cal. 2022) (discussing the scope of data involved in Google's bidding process).

95 *See* Ng, *supra* note 93.

96 *See id.*

97 *See* Annalee Monroe, *Fact Check: Does Facebook Sell Your Personal Data?*, AZ. REPUBLIC (Feb. 15, 2019), https://www.azcentral.com/story/news/politics/fact-check/2019/02/15/facebook-business-but-does-sell-your-personal-data/2701066002/ [https://perma.cc/2L6N-VHSK].

98 *Id.*; *see also* Michal Kosinski, *Congress May Have Fallen for Facebook's Trap, But You Don't Have To*, N.Y. TIMES (Dec. 12, 2018), https://www.nytimes.com/2018/12/12/opinion/facebook-data-privacy-advertising.html [https://perma.cc/5BUP-TFLU] (referring to Facebook's tactics in this regard as a "semantic trap").

data about the user along with "advanced machine-learning algorithms . . . [to] build predictive models for other sensitive traits, like religious and political views, personality, intelligence, sexual orientation, happiness, use of drugs or parental separation."[99] Children's ever-increasing online activities and digital trails could mean that predictive models using their data might be even more accurate than those developed for adults. Some advertisers may also use and store the information they collect during the real-time bidding process to create profiles and then subsequently sell it to third parties.[100] Google has been sued for allegedly allowing advertisers to access individuals' data through a real-time bidding auction process.[101]

Some child privacy advocates have described behavioral advertising as "manipulative and damaging for children."[102] Consider that researchers found that Meta would, for a mere three dollars, allow advertisers to target minors between the ages of thirteen and seventeen whose actions on its platforms indicated an interest in gambling and smoking.[103] A leaked 2017 Meta memo revealed that the company disclosed to advertisers that it could behaviorally target teenagers and identify when they "feel insecure,

---

[99] *Id.* For more on his argument, see Michal Kosinski et al., *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 PROCS. NAT'L ACAD. SCIS. 5802 (2013).

[100] *See* Kosinski, *supra* note 98; *see also* Joseph Cox, *Google Faces Class Action for Allegedly "Selling Users' Data"*, VICE (Mar. 29, 2021), https://www.vice.com/en/article/93we9z/google-class-action-lawsuit-real-time-bidding-selling-data [https://perma.cc/6PX5-9X9X] (discussing the litigation around Google's real-time bidding).

[101] *See In re* Google RTB Consumer Priv. Litig., 606 F. Supp. 3d 935; Cox, *supra* note 100; Allison Grande, *Google Hit with Privacy Suit over Data Shared in Ad Auctions*, LAW360 (Mar. 29, 2021), https://www.law360.com/articles/1369918/google-hit-with-privacy-suit-over-data-shared-in-ad-auctions [https://perma.cc/K5WS-D5AW]; Sara Merken, *Google Privacy Lawsuit over Ad Bidding Process to Go Forward*, REUTERS (June 14, 2022), https://www.reuters.com/legal/litigation/google-privacy-lawsuit-over-ad-bidding-process-go-forward-2022-06-14/ [https://perma.cc/KN9L-HKYN].

[102] Todd Feathers, *Debit Card Apps for Kids Are Collecting a Shocking Amount of Personal Data*, VICE (July 6, 2021), https://www.vice.com/en/article/4avqx3/debit-card-apps-for-kids-are-collecting-a-shocking-amount-of-personal-data [https://perma.cc/4LCN-6THF].

[103] *See* Josh Taylor, *Facebook Allows Advertisers to Target Children Interested in Smoking, Alcohol and Weight Loss*, GUARDIAN (Apr. 27, 2021), https://www.theguardian.com/technology/2021/apr/28/facebook-allows-advertisers-to-target-children-interested-in-smoking-alcohol-and-weight-loss [https://perma.cc/4LCN-6THF].

worthless, stressed, defeated, overwhelmed, stupid, silly, useless, and need a confidence boost."[104]

Children are particularly impressionable and are likely to be more vulnerable to companies' marketing tactics. Advertisements may quickly impact children's buying requests and desires.[105] Children may also be unable to easily identify "paid-for content" or understand how companies may use and monetize data collected about them and the possible repercussions of having their data in the hands of entities focused on increasing profits.[106] Similarly, a report by the American Psychological Association also notes that "most children younger than [seven to eight] years of age do not recognize the persuasive intent of commercial" advertisements.[107] Other studies also indicate that children have "fewer cognitive defenses against advertising than adults do."[108] One study on IoT smart speakers found that "young children ([five to seven] years old) attributed human-like qualities to the devices and developed an

---

104 JOSEFF, *supra* note 56, at 4 (internal quotes omitted).

105 *See* Joseph Jerome & Ariel Fox Johnson, *AdTech and Kids: Behavioral Ads Need a Time-Out*, COMMON SENSE 3 (2021), https://www.commonsensemedia.org/sites/default/files/uploads/pdfs/blog/adtech-and-kids-explainer.pdf [https://perma.cc/2Y66-92XE] ("[A]dvertising and marketing in general have a powerful effect on children. Studies demonstrate that ads quickly affect kids' desires and purchase requests, and parent-child conflicts can occur whenever parents or caretakers deny those requests precipitated by advertising.").

106 *See* MCCANN, *supra* note 14, at 2; BRIAN WILCOX ET AL., AM. PSYCH. ASS'N, REPORT OF THE APA TASK FORCE ON ADVERTISING AND CHILDREN 26 (2004), https://www.apa.org/pi/families/resources/advertising-children.pdf [https://perma.cc/LA3V-BYR5] (discussing children and advertising); *see also* Ariel Fox Johnson, *Behavioral Ads Are Bad for Kids*, COMMON SENSE (May 10, 2021), https://www.commonsensemedia.org/kids-action/articles/behavioral-ads-are-bad-for-kids [https://perma.cc/KJU4-V5GY] (arguing that children do not fully understand "how their data is collected, analyzed, and used").

107 WILCOX ET AL., *supra* note 106, at 5.

108 FAIRPLAY, GET THE FACTS: MARKETING AND MATERIALISM 1 (2021), https://fairplayforkids.org/wp-content/uploads/2019/10/materialism_fact_sheet.pdf [https://perma.cc/UF44-D7GK]; *see also* Stella C. Chia, *How Social Influence Mediates Media Effects on Adolescents' Materialism*, 37 COMMC'N RSCH. 400, 400-19 (2010); Marvin E. Goldberg & Gerald J. Gorn, *Some Unintended Consequences of TV Advertising to Children*, 5 J. CONSUMER RSCH. 22, 22-29 (1978); MCCANN, *supra* note 14, at 12; Suzanna J. Opree et al., *Children's Advertising Exposure, Advertised Product Desire, and Materialism: A Longitudinal Study*, 41 COMMC'N RSCH. 717, 717-35 (2013); Vanessa Vega & Donald F. Roberts, *Linkages Between Materialism and Young People's Television and Advertising Exposure in a US Sample*, 5 J. CHILD. & MEDIA 181, 181-93 (2011).

emotional attachment to them."[109] Over time, then, children could become addicted to interacting with IoT objects, which, if true, suggests that, for very young children, behavioral advertising conducted through these devices and related online services may have a significant adverse impact.

Additionally, even adults can have trouble distinguishing "third party widgets from first party content," and adults may not always "understand data flows . . . to third-party advertisers."[110] If this is true for adults, consider what this means for children subject to behavioral advertising online. An empirical study on online behavioral advertising concluded that some participants were not even aware that they were being subjected to behavioral advertisements, "never mind being aware of what data is collected or how it is used."[111]

There is also a close connection, in some cases, between social media platforms that frequently monetize user data and IoT objects. IoT data obtained by social media companies could potentially be used for targeted advertising. For example, Fitbit has previously allowed users to link their Fitbit accounts to their Facebook account to share fitness updates, thereby potentially allowing health-related data collected from the IoT device or mobile app to be shared with Meta.[112] Also recall that users of Amazon's Neighbors app can share Ring camera footage on social media. Owlet's privacy policy notes that its products incorporate "social media features, such as the Facebook 'Like' button," and use of those features will result in data collection by the social media company.[113] In other words, its

---

[109] Garg & Sengupta, *supra* note 57, at 2; *see* Thomas Claburn, *Study: How Amazon Uses Echo Smart Speaker Conversations to Target Ads*, REGISTER (Apr. 27, 2022), https://www.theregister.com/2022/04/27/amazon_audio_data/ [https://perma.cc/8WA3-HB6Y] (discussing how targeted ads can be placed on smart speakers); Katie Pray, *Targeting Ads on Smart Speakers, Smart Phones and Smart TVs, Are You Being Smart?*, VICI MEDI (June 1, 2020), https://vicimediainc.com/targeting-ads-on-smart-speakers-smart-phones-and-smart-tvs-are-you-being-smart/ [https://perma.cc/QSW2-AMEU] (detailing the same subject of targeted ads on smart technology).

[110] Aleecia M. McDonald & Lorrie Faith Cranor, *An Empirical Study of How People Perceive Online Behavioral Advertising* 6 (Carnegie Mellon Univ., CyLab-09-015, 2009).

[111] *Id.* at 20.

[112] *See* Elvy, *Commodifying Consumer Data*, *supra* note 28, at 445.

[113] *2018 Privacy Policy*, OWLET (July 20, 2018), https://owletcare.com/pages/privacy [https://perma.cc/9YZR-D2RP]. For all privacy policies, please refer to permalinks as those will reflect the versions from that moment, whereas the URLs may simply redirect to the current policy.

privacy policy implies that data collected via any such social media features would, for instance, in the case of Facebook, be governed by Meta's privacy policy.[114]

Research indicates that higher-income parents are more likely to evaluate the mobile apps downloaded by their children and are more knowledgeable about privacy concerns.[115] A 2020 study found that children from "lower-education households may be at higher risk of potential privacy violations . . . . [as] lower-education households had higher counts of data transmissions to a higher number of third-party domains."[116] These studies suggest that unequal access to privacy may become a growing concern, with children from lower-education households being more vulnerable to corporate data surveillance and monetization than children in higher-educated households.

iii. Anonymization and Aggregation Limits

As is the case with data collection and surveillance, companies' anonymization techniques can be used as a justification to allay concerns about child data monetizations as data collected by IoT devices and other sources can eventually be anonymized and aggregated.[117] For instance, Owlet's privacy policy states:

> We may anonymize or aggregate the information you provide and the information we collect through [our] Products, including personal information, and use it for any of the purposes we describe in this Privacy Policy. When we

---

114 *See id*. ("Your interactions with these features are governed by the privacy policy of the company providing them.").

115 *See* Zhao et al., *supra* note 86, at 2 ("Prior research suggests that parents with higher income are more likely to monitor the apps their children download and have more digital privacy knowledge and concerns."); Hwansoo Le, et al., *Information Privacy Concerns and Demographic Characteristics: Data from a Korean Media Panel Survey*, 36 GOV'T INFO. Q. 294, 294-303 (2019); Yong Jin Park, *Digital Literacy and Privacy Behavior Online*, 40 COMMC'N RSCH. 215, 215-36 (2011).

116 Zhao et al., *supra* note 86, at 1-2; *see also* Beata Mostafavi, *Some Children at Higher Risk of Privacy Violations from Digital Apps*, MICH. MED. (Sept. 8, 2020), https://www.michiganmedicine.org/health-lab/some-children-higher-risk-privacy-violations-digital-apps [https://perma.cc/LMH4-EBSM] (raising similar concerns).

117 *See* Ashutosh Bhagwat, *The Law of Facebook*, 54 U.C. DAVIS L. REV. 2353, 2385 (2021) (contending that "when social media firms sell advertising" the data is anonymized).

> anonymize or aggregate information, we remove any personal information that could be used by a third party to identify you and the child under your care from that information.[118]

Researchers have demonstrated that companies' anonymization techniques are not always effective.[119] One commentator notes

---

[118] *2020 Privacy Policy*, OWLET (last reviewed May 2024), https://owletcare.com/pages/privacy [https://perma.cc/QGG3-5EKN]; *see also 2023 Privacy Policy*, OWLET (last reviewed May 2024), https://owletcare.com/pages/privacy-policy [https://perma.cc/5UZ6-EB55] ("We may also provide third parties aggregate information, such as aggregate information regarding users of the Services, aggregate demographic information, and aggregated or anonymized information collected from the Services without restriction. For example, third parties may have access to information regarding the number of unique page requests, unique users of our Websites, and aggregate information on the types of activities users conducted while on our Websites.").

[119] *See Data Brokerage and Threats to U.S. Privacy and Security: Hearing on "Promoting Competition, Growth, and Privacy Protection in the Technology Sector" Before the Subcomm. on Fiscal Resp. & Econ. Growth*, 117th Cong. 6 (2021) (statement of Justin Sherman, Fellow and Research Lead, Data Brokerage Project) [hereinafter Statement of Justin Sherman] ("[R]esearchers unmasked supposedly anonymized ride data for New York City taxi drivers and could then calculate drivers' incomes."); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 704 (2016) ("For years, it was widely believed that as long as data sets were 'anonymized,' they posed no risk to anyone's privacy. If data sets were anonymized, then they did not reveal the identity of individuals connected to the data. Unfortunately, the notion of perfect anonymization has been exposed as a myth. Over the past twenty years, researchers have shown that individuals can be identified in many different data sets once thought to have been 'anonymized.'"); LUC ROCHER ET AL., ESTIMATING THE SUCCESS OF RE-IDENTIFICATIONS IN INCOMPLETE DATASETS USING GENERATIVE MODELS, 10 NATURE COMMC'NS 1, 2 (2019) ("Our results reject the claims that, first, re-identification is not a practical risk and, second, sampling or releasing partial datasets provide plausible deniability."); Quentin Fottrell, *A Worrying Theory After Equifax and Facebook Settlements – Aggregated Data Is NOT Enough to Protect Your Privacy*, MARKETWATCH (July 25, 2019), https://www.marketwatch.com/story/a-disturbing-theory-in-the-wake-of-the-equifax-settlement-anonymized-data-may-not-be-enough-to-protect-your-privacy-2019-07-23 [https://perma.cc/L7DD-L9DA] (discussing the limits of anonymization and aggregation); Linda Henry, *Is Anonymized Data Truly Safe from Re-Identification? Maybe Not*, JD SUPRA (Aug. 5, 2019), https://www.jdsupra.com/legalnews/is-anonymized-data-truly-safe-from-re-55837/ [https://perma.cc/DHQ2-SJMK] ("Although numerous prior studies have established that data anonymization is often reversible, the latest study demonstrates that technological advances have made it possible to de-anonymize data that might not have been previously possible, and it is becoming increasingly difficult to truly de-identify a data set and thus satisfy the requirements of privacy laws such as GDPR and the CCPA."); Natasha Lomas, *Researchers Spotlight the Lie of "Anonymous" Data*, TECHCRUNCH (July 24, 2019), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-

"[m]any studies have shown that individuals can be identified within anonymized and aggregated data sets."[120] One study using 1990 summary census data found that 87.1% of individuals could be identified by combining their gender, birth date, and zip code.[121] In 2021, seemingly anonymized and aggregated location cell phone data associated with mobile app usage obtained from a data vendor was used to reveal the alleged homosexual identity of a Catholic priest who later resigned from his position.[122] It is questionable whether certain types of data, such as precise location data and biometric data, can ever completely be anonymized in light of their inherent identifiable nature.[123] Similarly, several members of Congress have acknowledged the limits of anonymization and recommended that the FTC "define app developers' mislabeling of users' location data as 'anonymous' as a 'deceptive practice' through its Section 18 rulemaking authority."[124]

---

anonymous-data/ [https://perma.cc/RAK2-FTLD] (discussing the failures of anonymization).

120 Anonymous Editorial, *Digital-Data Studies Need Consent*, 572 NATURE 5, 5 (2019).

121 *See* Latanya Sweeney, *Uniqueness of Simple Demographics in the U.S. Population* (Lab'y for Int'l Data Priv., Working Paper LIDAP-WP4, 2000). Paul Ohm made this line of research accessible to lawyers. *See* Ohm, *supra* note 119, at 1719.

122 *See* Michelle Boorstein et al., *Top U.S. Catholic Church Official Resigns After Cellphone Data Used to Track Him on Grindr and to Gay Bars*, WASH. POST (July 21, 2021), https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/ [https://perma.cc/HYL4-EN2W]; Tim De Chant, *Catholic Priest Quits After "Anonymized" Data Revealed Alleged Use of Grindr*, ARSTECHNICA (July 21, 2021), https://arstechnica.com/tech-policy/2021/07/catholic-priest-quits-after-anonymized-data-revealed-alleged-use-of-grindr/?amp=1 [https://perma.cc/4BVD-XUBP] ("While this might be the first case of a public figure's online activities being revealed through aggregate data, 'it unfortunately happens very often' to the general public."); Carlos Gutierrez, *Outing of a Priest and Data Privacy in the LGBTQ Community*, BLADE (Aug. 12, 2021), https://www.washingtonblade.com/2021/08/12/opinion-outing-of-a-priest-and-data-privacy-in-the-lgbtq-community/ [https://perma.cc/296C-X335].

123 *See* Justin Banda, *Inherently Identifiable: Is It Possible to Anonymize Health and Genetic Data?*, IAPP (Nov. 13, 2019), https://iapp.org/news/a/inherently-identifiable-is-it-possible-to-anonymize-health-and-genetic-data/ [https://perma.cc/QSZ7-PZZ6] ("There is a growing skepticism in the field of data protection and privacy law that biometric data can never truly be deidentified or anonymized. This supposition rests on the fact that biometric data is inherently identifiable."); De Chant, *supra* note 122 ("When you're talking about location data, it's fundamentally not possible to have workable pseudonymity, because location data fingerprints are so revealing.").

124 Letter from Congress of the United States to Lina Khan, Chair, Fed. Trade Comm'n, & Jessica Rosenworcel, Chair, Fed. Commc'ns Comm'n (Dec. 9, 2021), https://raskin.house.gov/_cache/files/b/b/bba089eb-7b97-4b74-a7ad-f44cef5fd1bc/EA1DAC0E56C44CC379A28B713093351B.porter-raskin-location-

Even the FTC has acknowledged the weaknesses of anonymization in the behavioral advertising context.[125] An FTC staff report notes that a company could "collect anonymous tracking data" in connection with behavioral advertising and then connect that information to data that traditionally constitutes personally identifiable information ("PII"), such as a name or address, which the consumer may have provided during registration.[126] Further, new technological developments make it easier for companies to reveal an individual's identity, even if the data are anonymized.[127] As the FTC staff report observes, anonymized data "can become identifiable when combined and linked by a common identifier."[128] The staff report states that, "in the context of online behavioral advertising, the traditional notion of what constitutes PII versus non-PII is becoming less meaningful and should not, by itself,

---

data-privacy-letter-to-ftc-fcc.pdf [https://perma.cc/TSN6-GLR2] (recommending that the FTC view such practices as deceptive for location data). Some sources of privacy law in the United States exclude, de-identified and aggregated data from the definition of personal information. *See, e.g.*, CAL. CIV. CODE §1798.140 (West 2022). The CCPA defines de-identified data as data that "cannot reasonably be used to infer information about, or otherwise be linked to," an individual so long as the company that possesses the information adopts reasonable measures to prevent the data from being associated with an individual or household and "publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information." However, a company can attempt to reidentify the data to test "whether its deidentification processes satisfy" the CCPA's requirements and "contractually obligates any recipients of the" data to comply with the CCPA's de-identification requirements. Aggregate data is defined in the CCPA as data "that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device." *Id.*; *see also* David A. Zetoony, *Tomato, To-ma-toe: Is CCPA Deidentification the Same Thing as GDPR Anonymization?*, GREENBERG TRAURIG (Apr. 5, 2021), https://www.gtlaw-dataprivacydish.com/2021/04/tomato-to-ma-toe-is-ccpa-deidentification-the-same-thing-as-gdpr-anonymization/ [https://perma.cc/K3V3-9UHQ] ("The standard for 'deidentification' under the CCPA differs from the standard for 'anonymization' under the European GDPR. While the CCPA considers information that cannot 'reasonably' identify an individual as deidentified, the Article 29 Working Party interpreted European privacy laws as requiring that data has been 'irreversibly prevent[ed]' from being used to identify an individual.") (alteration in original).

125 *See* FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf [https://perma.cc/Y8C9-4AX3].

126 *Id.* at 22.

127 *See id.*

128 *Id.*

determine the protections provided for consumer data."[129] Additionally, in the case of shared IoT devices, such as in-home smart speakers, behavioral advertising based on users' interactions with such devices "could reveal private information to another" user in the same home, even if behavioral advertising does not clearly identify the user.[130]

With respect to aggregation, the FTC's former chief technologist and others have also recognized that group level aggregate data may be used to infer or deduce private information about an individual.[131] One study evaluating aggregate data associated with the online recommendation systems that companies like Amazon use found that these systems and related aggregate data can "leak information about the behavior of individual users."[132] American history would agree. For instance, the "aggregated, city-block level data" released by the Census Bureau helped identify the location of

---

[129] *Id.* at 21-22.

[130] *Id.* at 23.

[131] *See Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act Before the Comm. on the Judiciary*, 113th Cong. 5 (2013) (statement of Edward W. Felten, Professor, Princeton Univ.); Marc Rotenberg, Comment Letter on Proposed Consent Agreement with Compete, Inc. (Nov. 19, 2012), https://epic.org/wp-content/uploads/privacy/ftc/EPIC-FTC-Comments-Compete.pdf [https://perma.cc/9Z68-HKY8]; Ohm, *supra* note 119, at 1756 (discussing the limits and failures of data aggregation and contending that "even with interactive techniques and aggregation, data administrators cannot promise perfect privacy"); Ling Yin et al., *Re-Identification Risk Versus Data Utility for Aggregated Mobility Research Using Mobile Phone Location Data*, PLOS ONE, Oct. 2015, at 1, 1-20; Luk Arbuckle, *Aggregated Data Provides a False Sense of Security*, IAPP (Apr. 27, 2020), https://iapp.org/news/a/aggregated-data-provides-a-false-sense-of-security/ [https://perma.cc/X8QX-3ZAL] (discussing the differences between anonymized and aggregated data and noting that anonymized data can be aggregated and contending that various "forms of aggregation can be used to reconstruct the original data"); Victoria Mcintosh, *Understanding Aggregate, De-identified and Anonymous Data*, COMPARITECH (Oct. 25, 2019), https://www.comparitech.com/blog/information-security/aggregate-vs-anonymous-data/ [https://perma.cc/5S5Y-YCX3] ("[W]ith the right analysis, aggregate information can reveal significantly personal details"); HARSHA PANDURANGA ET AL., GOVERNMENT ACCESS TO MOBILE PHONE DATA FOR CONTACT TRACING 13 (2020), https://www.brennancenter.org/media/6068/download [https://perma.cc/N9QS-HZ4K] ("Although aggregate data conveys information about groups rather than individuals, it may be possible to identify individuals, especially if the data refers to a small geographic area or group, or if it is combined with publicly available information and examined over time.").

[132] Joseph A. Calandrino et al., *"You Might Also Like:" Privacy Risks of Collaborative Filtering*, IEEE SYMP. ON SEC. & PRIV., May 2011, at 231, 245.

Japanese Americans who were then transported to World War II internment camps.[133]

Other developments, such as differential privacy techniques that add "noise" via "positive and negative numbers" to hide and jumble individuals' data, may allow companies to identify useful trends from aggregate data while providing some level of privacy protection to individuals.[134] While differential privacy may be promising, its effectiveness depends in part on companies' willingness to adopt such techniques. Differential privacy also becomes applicable only after businesses have made decisions about what types of data and how much data they intend to collect.[135] Additionally, computer scientists have shown that the "dynamic behavior of high-dimensional aggregates like item similarity lists falls beyond the protections offered by any existing privacy technology, including differential privacy."[136]

The IoT may make true and vigorous data anonymization and aggregation strenuous to achieve.[137] The IoT is expected to generate "79.4 zettabytes . . . of data in 2025."[138] As we have seen, many of these IoT devices are directed towards children. IoT devices and associated systems also enable the collection of more detailed, specific, and potentially more accurate data about children's daily

---

133 Ohm, *supra* note 119, at 1756-57; *see* William Seltzer & Margo Anderson, Population Association of America, After Pearl Harbor: The Proper Role of Population Data Systems in Time of War (Mar. 28, 2000), https://pantherfile.uwm.edu/margo/www/govstat/newpaa.pdf [https://perma.cc/9P3B-HVKA] ("Even though the data did not identify particular houses or families, just telling authorities how many Japanese lived on each block gave them enough information to do enormous harm."). *Cf. with* JR Minkel, *Confirmed: The U.S. Census Bureau Gave Up Names of Japanese-Americans in WW II*, SCI. AM. (Mar. 30, 2007), https://www.scientificamerican.com/article/confirmed-the-us-census-b/ [https://perma.cc/7TQL-UHGX] (contending that the Census Bureau released more than just aggregated data).

134 Staff, *supra* note 67.

135 *See id.*; *Differential Privacy*, APPLE, https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf [https://perma.cc/ZN4U-XKNK] (last visited Oct. 19, 2022).

136 Calandrino et al., *supra* note 132.

137 *See* Guido Noto La Diega & Cristiana Sappa, *The Internet of Things at the Intersection of Data Protection and Trade Secrets Non-Conventional Paths to Counter Data Appropriation and Empower Consumers*, 3 EUR. J. CONSUMER L. 1, 14 (2020).

138 Carrie MacGillivray et al., *The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast*, BUS. WIRE (June 18, 2019), https://www.businesswire.com/news/home/20190618005012/en/The-Growth-in-Connected-IoT-Devices-is-Expected-to-Generate-79.4ZB-of-Data-in-2025-According-to-a-New-IDC-Forecast [https://perma.cc/VWT4-FXE9].

activities, habits, and lifestyle. This plethora of data permits companies to potentially obtain significant insights and make inferences about children's preferences beyond what is necessary to provide requested services. This concern is particularly true with respect to IoT wearable devices that "result in the availability of stable identifiers," which "lead to the creation of a unique fingerprint."[139] The increasing amount of more detailed data together with powerful algorithms may make it increasingly easy to re-identify children from anonymized data even as they age.

II. U.K. DESIGN CODE VERSUS CALIFORNIA DESIGN ACT

Recall that the California Design Act's preamble declares the legislature's intent to authorize firms covered by the Act to "look to guidance" issued under the U.K. Design Code when designing online products and services that children are likely to access.[140] The California Design Act authorizes the creation of the Children's Data Protection Working Group ("CDWG") and the legislature also expressed its intent that the CDWG consider the U.K. Design Code guidance issued by the United Kingdom's Information Commissioner's Office ("ICO") when creating best practices under the California Design Act.[141] Given this strong connection between the U.K. Design Code and the California Design Act, it is worth highlighting important differences and relative similarities between both frameworks, with a focus on evaluating the potential of the California Design Act to ameliorate the concerns discussed in Part I of this Article. The preamble of the bill on which the California Design Act is based notes that there is bipartisan consensus at the

---

139 La Diega & Sappa, *supra* note 137, at 15.

140 Assembly B. 2273, 2021-22 Gen. Assembly, Reg. Sess. (Cal. 2022) (enacted); *see* Explanatory Memorandum from the Department of Digital, Cultural, Media & Sport on the Age Appropriate Design Act 2020 (JUNE 11, 2020), https://www.gov.uk/government/publications/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020 [https://perma.cc/BJB6-Q7SN]; *see also* Charlotte Lunday, *How Cos. Can Adhere to New Calif. Kids Online Privacy Law*, LAW360 (Sept. 20, 2022), https://www.law360.com/cybersecurity-privacy/articles/1531917/how-cos-can-adhere-to-new-calif-kids-online-privacy-law?nl_pk=8bca81a9-bf53-40e6-b4c6-4d8c2eda4ebe&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy&utm_content=2022-09-21 [https://perma.cc/X2CD-7XYE].

141 *See* Cal. Assembly B. 2273.

international level, in California, and the United States that action must be taken in order to ensure that children can safely participate in the online world.[142] The decision to encourage reliance by both corporate actors and the CDWG on U.K. guidance[143] perhaps represents a new path towards transatlantic privacy law cooperation and harmonization enabled in part by collaborative governance.[144]

In addition to providing an in-depth comparative analysis of the U.K. Design Code and the California Design Act, this part also offers explanations for significant differences between both sources of law and evaluates potential challenges to the validity of the California Design Act, such as First Amendment and COPPA preemption concerns. The United Kingdom takes a fundamentally different approach than California in implementing the ideal of protecting children's privacy. This different approach is likely because data protection is viewed as a fundamental right in Europe in contrast to the consumer protection approach to data privacy adopted in the United States.

I argue that while the California Design Act may extend specific privacy protections to older minors, potentially cover personal information submitted both *from* and *about* minors, encourage the implementation of privacy and security by design and default, address some concerns with respect to datafication, surveillance and data monetization, the California Design Act's provisions could be interpreted to exclude physical IoT products from statutory protections. Additionally, it is not entirely clear whether limits on the use of personal information collected for age assurance purposes

---

142 *See id.*

143 These provisions appear to be contained in the non-binding legislative portions of the statute. *See id*. at § 1(d) ("It is the intent of the Legislature that businesses covered by the California Age-Appropriate Design Code may look to guidance and innovation in response to the Age-Appropriate Design Code established in the United Kingdom when developing online services, products, or features likely to be accessed by children."); *see also* Chris Micheli, *Are Legislative Findings and Declarations Necessary in Legislation?* CAL. GLOBE. (Oct. 11, 2020), https://californiaglobe.com/articles/are-legislative-findings-and-declarations-necessary-in-legislation/ [https://perma.cc/4UTC-SYB5] (noting that in California the "legislative findings and declarations" section of bills "are the equivalent of a preamble").

144 On the issue of collaborative governance, Margot Kaminski contends that "the GDPR is both a system of individual rights and a complex compliance regime that, when applied to the private sector, is constituted through collaborative governance." Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CALIF. L. REV. 1529, 1583 (2019).

will effectively address concerns about children's anonymity and privacy.

This section also exposes important similarities and differences between the California Design Act and COPPA which may impact the reach and effectiveness of the California Design Act. Many of the indicators used in the California Design Act to determine whether an entity is subject to the Act are similar to those found in COPPA's framework. Further, assuming that the California Design Act survives the ongoing legal challenge, absent similar legislative action in more states or voluntary corporate extension of similar protections under the California Design Act to children in other states, children who reside in California may have more privacy protections than those in other states. This potential reality also raises unequal access to privacy concerns as the level of privacy protection that children will receive could depend on where they happen to reside and, oftentimes, children have little to no control over where they reside. Recall that Maryland recently adopted a law modeled in part on the California Design Act.

a. Notable Differences

There are several seemingly important differences between the U.K. Design Code and the California Design Act. This section highlights four key areas in which both frameworks differ. First, both frameworks have different underlying principles, with the U.K. Design Code's animating instruments recognizing privacy as a fundamental right and the California Design Act's related instruments adopting a consumer protection approach to privacy. Second, while the U.K. Design Code and the California Design Act both rely primarily on governmental actors to enforce each framework, the California Design Act expressly excludes private rights of action, whereas the U.K. Design Code does not appear to disturb the pre-existing ability of individual claimants to bring civil claims for violations under foundational sources of law. Unlike the U.K. Design Code which is a "code of practice" that sheds light on the application of pre-existing U.K. data protection law, the California Design Act is a statute.[145] Third, the U.K. Design Code

---

[145] Lesley Hannah & Kio Gwilliam, *The Age Appropriate Design Code: Strong on Principles But Will It Trigger Change?*, HAUSFELD FOR CHALLENGE (Sept. 22, 2021), https://www.hausfeld.com/nl-nl/what-we-think/perspectives-blogs/the-age-

appears to have a broader scope than the California Design Act's approach, with the later seeming to be in keeping with COPPA's scope in some instances. Lastly, the U.K. Design Code encourages age verification while the California Design Act contains age estimation provisions.

i. Distinct Foundational Principles

The U.K. Design Code and the California Design Act have different foundational principles. The U.K. Design Code was born out of the United Kingdom's Data Protection Act of 2018 ("U.K. DPA").[146] The U.K. DPA required the ICO, "an independent supervisory authority,"[147] to create "a code of practice" to provide "guidance [on] . . . appropriate standards of age-appropriate design of relevant information society services which are likely to be accessed by children."[148] The term "relevant information society services" is defined, in part, in the U.K. DPA as services involved in personal data processing under the European Union's ("EU") General Data Protection Regulation ("GDPR").[149] Once prepared, the ICO submitted the code to the Secretary of State who, in turn, presented the code to Parliament.[150] In issuing the code, the ICO was

---

appropriate-design-code-strong-on-principles-but-will-it-trigger-change/ [https://perma.cc/M7UV-283H] ("The Code is "*not a new law*" but, rather, sets standards and gives greater clarity on the interpretation of the UK GDPR in so far as it applies to children's data.").

146 *See* DATA PROTECTION ACT 2018, c. 12 (UK). In addition to the U.K. Design Code, the Irish Data Protection Commission has also published its own guidance, "Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing," on child privacy which shares some similarities and differences with the U.K. Design Code. IR. DATA PROT. COMM'N, *supra* note 1 (discussing same and noting that the U.K. DPA of 2018 "gives effect in Irish Law to the GDPR").

147 DATA PROTECTION ACT 2018, c. 12, sch. 3, pt. 5, sch. 6, pt. 1, sec. 40 (UK).

148 *Id*. *cf*. 12, pt. 5, sec. 123.

149 *Id*. *cf*. U.K. DESIGN CODE, *supra* note 1, at 15-16 (positing that the U.K. Design Code applies to the "relevant information society services" discussed in the U.K. DPA) *with* Regulation 2016/679 of Apr. 27, 2016, General Data Protection Regulation, 2016 O.J. (L 119) art. 4(25) [hereinafter GDPR] ("[I]nformation society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council"); *see also* Directive 2015/1535, of the European Parliament and of the Council of 9 September 2015 Laying Down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society Services (codification), 2015 O.J. (L 241) 1, 3 (defining "information society service").

150 *See* DATA PROTECTION ACT 2018, c. 12, pt. 5, sec. 125 (UK).

obligated to consider the different developmental needs of children based on their age as well as the United Kingdom's obligations under the United Nations Convention on the Rights of the Child ("UNCRC").[151] In contrast, to date, the United States has not yet ratified the UNCRC.[152]

The U.K. Design Code is grounded in the GDPR. More specifically, the U.K. DPA is the United Kingdom's "implementation" of the GDPR, although the GDPR has direct effect in member states.[153] The GDPR is no longer applicable in the United Kingdom post-Brexit, but the United Kingdom kept the GDPR in U.K. law with some adjustments via the U.K. General Data Protection Regulation ("U.K. GDPR"), which "sits alongside [and supplements] an amended version of the" U.K. DPA.[154] The U.K.

---

[151] *See id*. c. 12, pt. 5, sec. 123(4); Convention on the Rights of the Child, Sept. 2, 1990, 1577 U.N.T.S. 27531.

[152] *See* Sarah Mehta, *There's Only One Country in the World That Has Failed to Ratify the Convention on the Rights of the Child: US*, AM. C.L. UNION https://www.aclu.org/news/human-rights/theres-only-one-country-hasnt-ratified-convention-childrens [https://perma.cc/K9G6-665W].

[153] *The Data Protection Act*, UK GOV'T, https://www.gov.uk/data-protection [https://perma.cc/5SQR-MHTD] (last visited Oct. 24, 2022); INFORMATION COMM'R'S OFF., AN OVERVIEW OF THE DATA PROTECTION ACT 2018 4 (2019), https://ico.org.uk/media/for-organisations/documents/2614158/ico-introduction-to-the-data-protection-bill.pdf [https://perma.cc/U3N5-VXKD] ("The [U.K. DPA] does not write the GDPR into [U.K.] law. The GDPR has direct effect in EU member states from 25 May 2018, which means the GDPR is already part of [U.K.] law. After the [United Kingdom] leaves the EU, the GDPR will be converted into [U.K.] law (with some amendments) under the European Union (Withdrawal) Act 2018. However, the GDPR permits Member States to make some adaptations to reflect national requirements.").

[154] *The U.K. GDPR*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/ [https://perma.cc/J37L-8VBW] (last visited June 5, 2024). The U.K. DPA "was amended on 1 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the [United Kingdom]'s status outside the EU." INFORMATION COMM'R'S OFF., INTRODUCTION TO DATA PROTECTION 7 (2022), https://ico.org.uk/media/for-organisations/guide-to-data-protection/introduction-to-dpa-2018-1-0.pdf [HTTPS://PERMA.CC/BS5U-FMU6]. As far as sitting "alongside and supplement[ing]" the U.K. GDPR, it does so by providing "exemptions," setting forth "separate data protection rules for law enforcement authorities, extend[ing] data protection to some other areas such as national security and defen[s]e, and set[ting] out the Information Commissioner's functions and powers." *Id.* By comparison, the U.K. GDPR "sets out the key principles, rights and obligations for most processing of personal data in the [United Kingdom], except for law enforcement and intelligence agencies." *Id.*; *see also Brexit and Data Protection in the UK*, IT GOVERNANCE, https://www.itgovernance.co.uk/eu-gdpr-uk-dpa-2018-uk-gdpr [https://perma.cc/HM68-SBDY] (last visited Oct. 22, 2022) ("[W]ith effect from 1 January 2021, the [Data Protection, Privacy and Electronic Communications]

ICO has noted that "in practice, there is little change to core data protection principles" since Brexit.[155] Similarly, in connection with the issuance of the adequacy decision permitting the free flow of data between the EU and the United Kingdom post-Brexit, the European Commission stated that the United Kingdom's "data protection system continues to be based on the same rules that were applicable when the [United Kingdom] was a Member State of the EU [as] the [United Kingdom] has fully incorporated the principles, rights and obligations of the GDPR . . . into its post-Brexit legal system."[156] Of course, the United Kingdom may eventually depart from the GDPR model by adopting amendments to its existing privacy regimes, which could impact the U.K. Design Code.[157]

California has long been a super privacy regulator. The California Design Act is in keeping with this position. California is the first state to adopt a broad state privacy law statute—the CCPA. The CCPA spurred legislation in other states and reignited privacy debates at the federal level—the so called "California Effect."[158] Just as the U.K. DPA and the GDPR serve as the U.K. Design Code's animating documents, the CCPA and its 2020 amendments do the

---

Regulations *have* amended the DPA 2018 to merge it with the requirements of the EU GDPR, forming a new, U.K.-specific data protection regime that will work after Brexit."); *Differences Between the UK-GDPR and the EU-GDPR Regulation*, GDPR EU, https://www.gdpreu.org/differences-between-the-uk-and-eu-gdpr-regulations/ [https://perma.cc/R433-C2GW] (last visited Oct. 20, 2022) (discussing the differences).

155 *OVERVIEW—DATA PROTECTION AND THE EU*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/#GDPR (last visited Oct. 20, 2022) [https://perma.cc/8KUR-Q4WA] ("The EU GDPR is an EU Regulation and it no longer applies to the [United Kingdom].").

156 Press Release, European Commission, Data Protection: Commission Adopts Adequacy Decisions for the UK (June 28, 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183 [https://perma.cc/E263-EE78].

157 *See* Leigh Mallon, *UK Government Announces Extensive Post-Brexit Changes to Data Privacy Laws*, STEPTOE (May 11, 2022), https://www.steptoe.com/en/news-publications/uk-government-announces-extensive-post-brexit-changes-to-data-privacy-laws.html [https://perma.cc/UUV2-62LJ] (discussing proposed changes to U.K. GDPR and U.K. DPA that would differ from GDPR requirements); Rachel Wolcott, *UK Announces Data Reform Bill to Reduce Compliance Burden and Ease Reuse for Research*, THOMSON REUTERS (May 31, 2022), https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/uk-data-reform-bill/ [https://perma.cc/ZZ7L-LZRK] (discussing proposed changes to UK privacy law).

158 Anupam Chander et al., *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1742 (2021).

same to some extent for several aspects of the California Design Act. Indeed, in the uncodified preamble of the California Design Act, the legislature declared that the Act furthers the aims and purposes of the 2020 amendments to the CCPA.[159] The California Design Act also seemingly relies on the CCPA's pre-existing definitions of several terms, such as "precise geolocation" and "businesses."[160] The California Design Act relies on the California Privacy Protection Agency to appoint some members of the CDWG.[161] Although the CCPA is distinct from the GDPR in notable ways, there are several similarities between both sources of law.[162]

One might view the California legislature's decision to use the U.K. Design Code as a model as a strategic move in keeping with the American legal system's early reliance on British law.[163] The California Design Act arguably evidences the influence and reach of the GDPR and the so-called Brussels Effect. The U.K. Design Code, upon which the California Design Act is based, has its roots in the GDPR. Additionally, the California Design Act's reliance on the U.K. Design Code is perhaps a continuation of both legal systems' previous history of adopting laws based on and in response to legal innovation in each jurisdiction. For instance, the United Kingdom's Modern Slavery Act of 2015, described by some as the first law "of

---

159 *See* Assembly B. 2273, 2021-22 Gen. Assembly, Reg. Sess. (Cal. 2022) (enacted).

160 CAL. CIV. CODE § 1798.99.30 (West 2023) ("For purposes of this title, the definitions in Section 1798.140 shall apply unless otherwise specified in this title."); James Sullivan et al., *California's Age-Appropriate Design Code Act- and the Looming State Patchwork of Online Child Protection Laws*, DLA PIPER (May 8, 2023), https://www.dlapiper.com/en/insights/publications/2023/05/californias-age-appropriate-design-code-act#:~:text=Collecting%2C%20selling%2C%20or%20sharing%20precise,that%20such%20activity%20is%20necessary) [https://perma.cc/6WNT-XJ4K] ("The CAADCA applies to companies that (1) meet the definition of a "business" under the California Consumer Privacy Act (CCPA) and (2) develop and provide an "online service, product, or feature" (Online Service) that is "likely to be accessed" by consumers who are under 18 years of age.").

161 *See* Assembly B. 2273, 2021-22 Gen. Assembly, Reg. Sess. (Cal. 2022) (enacted).

162 *See* Chander et al., *supra* note 158, at 1746, 1749-55; Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 810 (2019).

163 *See, e.g.*, Herbert Pope, *English Common Law in the United States*, 24 HARV. L. REV. 6 (1910) (DISCUSSING INFLUENCE OF ENGLISH COMMON LAW IN THE UNITED STATES); William B. Stoebuck, *Reception of English Common Law in the American Colonies*, 10 WM. & MARY L. REV. 393 (1969) (examining the same).

its kind in Europe," borrows significantly from the California Transparency in Supply Chain Act of 2010.[164]

Despite use of the U.K. Design Code as a model, the California Design Act and the CCPA do not appear to view data protection or privacy as a fundamental or human right in the same manner that the GDPR does.[165] The United Kingdom and the EU recognize a fundamental right to data privacy in accordance with the European Convention on Human Rights; the United Kingdom also acknowledges children's right to privacy via the UNCRC.[166] This fundamental right is not just limited to consumer transactions. As notable legal scholars have observed, the European approach to

---

[164] MAUREEN GORSEN, UK FOLLOWS CALIFORNIA LEAD IN HOLDING COMPANIES RESPONSIBLE FOR SLAVERY IN SUPPLY CHAIN (2014), https://www.alston.com/-/media/files/insights/publications/2015/06/ichemical--product-regulation-advisoryi-uk-follows/files/view-advisory-as-pdf/fileattachment/g15375-uk-supply-chain-slavery.pdf [https://perma.cc/KN9J-6USG].

[165] *See* Chander et al, *supra* note 158, at 1755-56.

[166] *See* European Convention on Human Rights, Nov. 4, 1950, Eur. T.S. No. 5, 213 U.N.T.S. 221; Charter of Fundamental Rights of the European Union, arts. 7, 8, 2012 O.J. (C 326) 2; *Data Protection*, EUR. DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection_en (last visited Feb. 2, 2020) [https://perma.cc/E263-EE78]; Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115 (2017) ("European Convention of Human Rights is not part of the EU, but a normal international treaty. It binds the contracting states as part of the body of international law . . . [but the] the EU applies the Convention as far as they constitute general principles of the Union's law . . . . The Convention established the European Court of Human Rights, which has built on Article 8 to identify specific rights regarding data protection."); INFORMATION COMM'R'S OFF., INTRODUCTION TO DATA PROTECTION 3 (Oct. 14, 2022), https://ico.org.uk/media/for-organisations/guide-to-data-protection/introduction-to-dpa-2018-1-0.pdf [https://perma.cc/S3FW-4AVX] ("[D]ata protection is the fair and proper use of information about people. It's part of the fundamental right to privacy – but on a more practical level, it's really about building trust between people and organi[z]ations."); EUROPEAN COURT OF HUMAN RIGHTS, GUIDE TO CASE-LAW OF EUROPEAN COURT OF HUMAN RIGHTS (Dec. 31, 2020), https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0n [https://perma.cc/NF93-WFP4]; MINISTRY OF JUSTICE, HUMAN RIGHTS: THE UK'S INTERNATIONAL HUMAN RIGHTS OBLIGATIONS (last updated Mar. 30, 2022), https://www.gov.uk/government/collections/human-rights-the-uks-international-human-rights-obligations [https://perma.cc/HK9E-A6SK] (noting that the United Kingdom has ratified the European Convention on Human Rights); Brian Mund, *Can Britons' Data Privacy Be Protected After Brexit?*, YALE J. INT'L L., https://www.yjil.yale.edu/can-britons-data-privacy-be-protected-after-brexit/#_ftnref16 [https://perma.cc/8A7T-4YWE] (last visited June 5, 2024); *The United Nations Convention on the Rights of the Child and What It Means for Online Services*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/childrens-code-hub/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/the-united-nations-convention-on-the-rights-of-the-child/#impact [https://perma.cc/2WQK-TL7D] (last visited Oct. 20, 2022).

privacy "places data protection rights on the same plane as free speech or due process."[167] At the state level, there has been at least one legislative proposal to enact a data protection statute that would facilitate the creation of a privacy bill of rights that includes an express right to data protection.[168]

As Neil Richards and Woodrow Hartzog have convincingly argued, "in the United States, consumer privacy rules implement public policy, but they do not enforce fundamental rights of privacy."[169] While Europe has focused on data protection and the principle that individuals' data must not be processed or collected without a legal justification, U.S. privacy law has often relied on a consumer protection approach.[170] Under this approach, regulators are primarily concerned with notice and choice and ensuring that firms provide consumers with the contracted-for bargain.[171] The United States also historically adopted a sectoral approach to privacy. In contrast, "in every European nation, specialized data protection regulators have long enforced omnibus statutes

---

[167] Chander, et al., *supra* note 158, at 1747; *see* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1727, 1730 (2020) (discussing the differences between the GDPR and U.S. approach to freedom of expression and contending that "the American constitutional system has no explicit constitutional right to privacy" and that in the United States, "the fundamental right of free expression protected by the First Amendment is not subject to [a] proportionality analysis").

[168] *See* Assembly B. 3005, 2021-22 Leg. Sess. (N.Y. 2021) ("Consumers shall have the following rights: (a) the right to protection of their personal information by covered entities."); *Protecting Data Privacy and Innovation*, U.S. Chamber Com., (2022), https://www.uschamber.com/data-privacy [https://perma.cc/J4VY-HYT9] ("The 'New York Data Accountability and Transparency Act' would task the Secretary of State through rulemaking to develop a Privacy Bill of Rights including but not limited to the right to data protection, access, correction, deletion, control, and opting out of sales. A new Data Privacy Advisory Board would provide guidance. Both bills 'have been recommitted to their respective finance committees.'"); *see also* Alejandro Cruz & Christina Seda-Acosta, *New York Has More to Say About Consumer Data Privacy*, JD SUPRA (Feb. 10, 2021), https://www.jdsupra.com/legalnews/new-york-has-more-to-say-about-consumer-9071107/ [https://perma.cc/TC4H-PGMU] (describing the New York Data Accountability and Transparency Act as a "comprehensive data privacy law").

[169] Hartzog & Richards, *supra* note 167, at 1728 ("European consumer privacy law is built upon a foundation of fundamental human rights that are protected against both governments and private actors; American consumer privacy law is not.").

[170] *See* Chander, et al., *supra* note 158, at 1747-48.

[171] *See id.*

applicable to all organizations when they handle any personal data."[172]

The CCPA also takes a largely consumer protection approach to privacy despite some similarities with the GDPR and the state constitutional inalienable right to privacy.[173] The GDPR finds its roots in the principle of lawful processing, which is at "the core of" European data protection law.[174] Under this concept, an individual's personal data should not be processed unless one of six lawful bases for processing is satisfied.[175] These include opt-in consent and legitimate interests.[176] In contrast, the CCPA does not obligate companies to first satisfy a lawful basis for data processing but instead presumes that consumer data may be collected and monetized absent legal rules restricting such practices.[177]

As Margot Kaminski and others observe, the CCPA "remains in the American tradition, a transactional privacy law concerned with

---

[172] *Id*. at 1748.

[173] *See id*.; CAL. CONST. ART. I, § 1; Donorovich-Odonnell v. Harris, 241 Cal. App. 4th 1118, 1139 (2015) ("Not only is the state constitutional right of privacy embodied in explicit constitutional language not present in the U.S. Constitution, but past California cases establish that, in many contexts, the scope and application of the state constitutional right of privacy is broader and more protective of privacy than the federal constitutional right of privacy."); Golden Data Law, *California's Constitutional Right to* Privacy, MEDIUM (Oct. 15, 2020), https://medium.com/golden-data/the-californias-constitutional-right-to-privacy-4a1900d11ee8 [https://perma.cc/MMS3-WTZK] ("California's right to privacy is wider than it's federal counterpart in that it protects individuals not only against violations by state and federal government entities, but also against violations by other individuals and private companies."); *see also* Mark Smith, *California Privacy Reboot Puts Rights in Spotlight*, BLOOMBERG L. (Jan. 15, 2021), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-california-privacy-reboot-puts-rights-in-spotlight [https://perma.cc/4NXH-RJ2F] ("California's constitution specifically recognizes privacy as an "inalienable" right, and it is the only state constitution to elevate privacy to such a status."); *see also* David A. Carrillo et al., *California Constitutional Law: Privacy*, 59 SAN DIEGO L. REV. 119 (2022) (arguing for a return of the compelling need test to create a more robust interpretation of the California constitutional right to privacy and contending that the CCPA's coverage of only certain businesses illustrates its narrower focus and the need to expand current limited interpretations of the California constitutional right to privacy); Grace Park, *The Changing Wind of Data Privacy Law: A Comparative Study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act*, 10 U.C. IRVINE L. REV. 1455 (discussing the history of the California constitutional right to privacy).

[174] Chander et al., *supra* note 158, at 1756.

[175] *See id.;* GDPR art. 6(1)(a)-(f).

[176] *See id*.

[177] *See* Chander et al., *supra* note 158, at 1756-77; CAL. CIV. CODE § 1798.100 (West 2020).

protecting [individual citizens as] *consumers* in their dealings with *commercial* entities."[178] One California court has noted that "the CCPA is a statute that is focused on particular practices; namely, it seeks to address the sale of [personal information ("PI")] and the disclosure of PI for business purposes."[179] Similarly, the California Design Act is also focused on protecting children in their online interactions with businesses whose services and products they are likely to access. In keeping with a consumer protection approach, the uncodified preamble of the California Design Act notes that "children are particularly vulnerable from a negotiating perspective with respect to their privacy rights" in their dealings with companies.[180]

The California Design Act could also influence lawmakers in other states and change the way that businesses operate in other states. The California Design Act has already inspired similar legislation in New York. [181] Companies could decide to extend the protections under the California Design Act to children in other states to decrease the operational load. However, if the California Design Act survives the ongoing legal challenge, absent the enactment of similar legislation in other states or voluntary corporate extension of similar protections to children in other states, children who reside in California and in states that adopt similar laws may have more privacy protections than those in other states. This potential reality could contribute to unequal access to privacy between children who are citizens of different states. BIPA presents a similar problem. While consumer protection legislation varies from state to state, the internet is borderless and today's children face unprecedented datafication, surveillance and monetization risks when compared to previous generations.

---

178 Chander et al., *supra* note 158.

179 Kaupelis v. Harbor Freight Tools USA, Inc., 2020 WL 7383355, at *2 (C.D. Cal. Sept. 28, 2020) (alteration in original).

180 Assembly B. 2273, 2021-22 Gen. Assembly, Reg. Sess. § 1(a)(9) (Cal. 2022) (enacted).

181 *See* Allison Grande, *Calif.'s Novel Privacy Moves May Dim Federal Law's Chances*, LAW360 (Oct. 5, 2022), https://www.law360.com/cybersecurity-privacy/articles/1537006/ [https://perma.cc/4GDR-XWKD].

ii. Methods of Enforcement

The U.K. Design Code and the California Design Act rely on government actors to serve as the core actors responsible for enforcement. However, the California Design Act expressly excludes a private right of action, while the U.K. Design Code does not appear to disturb the pre-existing ability of individual claimants to bring civil claims for violations of U.K. privacy law.[182] This is perhaps because of the difference in the nature of the instruments, with one being a traditional statute and a primary source of law and the other a statutory code of practice (originating from a legal mandate in a pre-existing source of law), not to mention overarching differences in each legal system's approach to privacy protection.[183]

The California Design Act is to be enforced exclusively by the state attorney general and businesses who violate the Act may be

---

[182] *See* CAL. CIV. CODE § 1798.99.35(d) (West 2022); U.K. DESIGN CODE, *supra* note 1, at 12.

[183] *See* U.K. DESIGN CODE, *supra* note 1, at 4 ("The code is not a new law but it sets standards and explains how the [GDPR] applies in the context of children using digital services."); Adele Harrison, *UK's Age Appropriate Design Code in Effect*, ORRICK (July 26, 2021), https://www.orrick.com/en/Insights/2021/07/The-UKs-Age-Appropriate-Design-Code-Comes-into-Force-in-September-2021 [https://perma.cc/7436-TCUB] ("[A]lthough the [UK Design] Code itself is not law . . . ."); Stephens Scown, *Providers of Online Services – Are You Ready for the Children's Code?*, STEPHENS SCOWN (Sept. 27, 2021), https://www.stephens-scown.co.uk/intellectual-property-2/data-protection/providers-of-online-services-are-you-ready-for-the-childrens-code/ [https://perma.cc/T4GS-HPUB] ("Whilst the Children's Code is not law . . . ."); Harriet Parratt, *Age Appropriate Design Code Boosts Protection of Children's Data*, OSBORNE CLARKE (Feb. 18, 2021), https://www.osborneclarke.com/insights/age-appropriate-design-code-boosts-childrens-data-protection [https://perma.cc/9RQB-7PRJ] ("The code is not law, however, it carries significantly more weight than guidance."); Tom Phipps et al., *ICO's Children Code*, ASHFORDS (Feb. 21, 2022), https://www.ashfords.co.uk/news-and-media/general/the-ico-s-children-s-code [https://perma.cc/656T-YW2F] ("Whilst [the U.K. Design Code] is not law, in practice, in the event of a complaint (such as an allegation of a data breach), the courts and the ICO will take the Code and compliance with it into account.") (alteration in original); Leanne Yendell, *The Children's Code – Does Your Website or Platform Comply?*, STEPHENS SCOWN (Sept. 29, 2021), https://www.stephens-scown.co.uk/intellectual-property-2/the-childrens-code-does-your-website-or-platform-comply/ [https://perma.cc/C4BF-ZVVU] (noting that the [U.K. Design] Code "is not law"); *Safeguarding Children Online: ICO Publishes Code of Practice*, SLAUGHTER & MAY (Jan. 22, 2020), https://thelens.slaughterandmay.com/post/102fx9u/safeguarding-children-online-ico-publishes-code-of-practice [https://perma.cc/E85U-QFWT] (The U.K. Design Code "is not law but is required by the Data Protection Act 2018 and carries more weight than a simple ICO guidance piece.").

subject to an injunction and civil penalties of "not more than two thousand five hundred dollars ($2,500) per affected child for each negligent violation or not more than seven thousand five hundred dollars ($7,500) per affected child for each intentional violation."[184] The California Design Act notes that the Act should not be interpreted to "serve as the basis of a private" cause of action under any other source of law.[185]

The lack of a private right of action is a significant drawback under the California Design Act. Private rights of action are an important enforcement tool that can encourage companies to comply with their legal obligations. Governmental entities often have limited resources, so they may not always timely hold corporate actors liable for statutory violations. BIPA illustrates the value of private rights of action in a law that relies in part on notice-and-consent mechanisms for data collection. Other states with biometric data statutes that lack a private right of action, such as Washington and Texas, have seen comparatively less enforcement by their state attorneys general.[186] BIPA lawsuit settlements have resulted not only in monetary compensation but also in limiting corporate actors' ability to provide facial recognition software to other entities.[187]

The U.K. Design Code does not appear to be an authoritative statement of law in the traditional sense. Under the U.K. DPA, a company's failure to comply with a code "*does not of itself make [the*

---

184 CAL. CIV. CODE § 1798.99.35 (West 2022).

185 *Id.*

186 *See* Rachel Metz, *Here's Why Tech Companies Keep Paying Millions to Settle Lawsuits in Illinois*, CNN BUS. (Sept. 20, 2022), https://www.cnn.com/2022/09/20/tech/illinois-biometric-law-bipa-explainer/index.html [https://perma.cc/CTF6-UCHR] (Texas and Washington's biometric data "laws have hardly been tested (in 2022, Texas, also sued Facebook over allegations that it illegally snagged Texans' facial-recognition data), likely because it's up to the state, rather than individual citizens, to decide whether to sue."); *see also* Elvy, *Commodifying Consumer Data*, *supra* note 28, at 429; Kashmir Hill & David McCabe, *Texas Sues Google for Collecting Biometric Data Without Consent,* N.Y. TIMES (Oct. 20, 2022), https://www.nytimes.com/2022/10/20/technology/texas-google-privacy-lawsuit.html [https://perma.cc/BQV7-SG8B] (discussing Texas' 2022 suit against Google for the collection of biometric data via its Nest Cameras and other services without consent).

187 *See* Metz, *supra* note 186; Rachel Metz, *Clearview AI Agrees to Restrict US Sales of Facial Recognition Mostly to Law Enforcement*, CNN BUS. (May 9, 2022), https://www.cnn.com/2022/05/09/tech/clearview-ai-aclu-settlement/index.html [https://perma.cc/K3PY-MASA].

company] liable [in] legal proceedings in a court or tribunal."[188] The text of the U.K. Design Code states that "[o]rgani[z]ations should conform to the code and demonstrate that their services use children's data fairly."[189] The U.K. DPA provides that the ICO must consider the U.K. Design Code in determining compliance with privacy requirements under U.K. law and conformance with the code can serve "as admissible . . . evidence in legal proceedings."[190] The text of the U.K. Design Code acknowledges this and notes that "courts must take its provisions into account wherever relevant."[191] The ICO also indicated that covered entities who fail to satisfy the requirements of the U.K. Design Code may find it onerous to prove compliance with their legal obligations under U.K. privacy law and "may invite regulatory action" as a result.[192] The ICO intends to monitor compliance through complaint investigations and proactive audits.[193]

Notably, as U.K. legal practitioners have argued, individual claimants and public interest groups can rely on the U.K. Design Code when asserting civil claims for violations of the U.K. GDPR and "the U.K. DPA envisages this" possibility.[194] Individuals have the right to compensation under U.K. privacy law for damages resulting from violations of privacy rights and these right can be

---

188 DATA PROTECTION ACT 2018 c. 12, pt. 5 § 127 (UK).

189 U.K. Design Code, *supra* note 1, at 4.

190 DATA PROTECTION ACT 2018 c. 12, pt. 5 § 127 (UK).

191 U.K. Design Code, *supra* note 1, at 12.

192 *See ABOUT THIS CODE*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/about-this-code/?q=new+law (last visited Mar. 19, 2024) [https://perma.cc/7TEX-9MJZ].

193 *See* Parratt, *supra* note 183.

194 Harrison, *UK's Age Appropriate Design Code in Effect*, *supra* note 183 ("[I]ndividual claimants and representative actions, will also seek to rely on the Code when bringing civil claims alleging noncompliance with the UK GDPR . . . [A]lthough the [U.K. Design] Code itself is not law, a breach of the Code may form the evidential basis for a successful argument [under the] [U.K.] GDPR and any breach of [the] [U.K.] GDPR may lead to significant enforcement actions, regulatory fines and civil claims."); Yendell, *supra* note 183 ("Whilst the [U.K. Design] Code itself is not law, the [ICO] will take this Code into account, along with other relevant legislation, when considering whether you have complied with data protection laws. The Code can also be used in evidence in court proceedings, and the courts must take its provisions into account wherever relevant. If you do not meet the requirements under the legislation, you are at risk of sizable fines under the [ICO] enforcement powers and potential civil action.").

enforced in court.[195] With respect to the ICO's enforcement powers, although the ICO has received criticism for its seeming unwillingness to use its enforcement powers effectively for serious violations of data protection principles, the ICO has "the power to issue fines of up to £17.5 million . . . or 4% of [a company's] annual worldwide turnover, whichever is higher."[196]

iii. Scope

Subject to some exceptions, the U.K. Design Code applies to "information society services . . . likely to be accessed by children" and the California Design Act applies to a "business that provides an online service, product, or feature likely to be accessed by children."[197] The California Design Act does not define the term "business," but instead, as mentioned earlier, relies on the CCPA's definition.[198] At first glance, the use of the term "likely to be

---

[195] *See CAN THE RIGHT OF ACCESS BE ENFORCED?*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/can-the-right-of-access-be-enforced/ (last visited Mar. 19, 2024) [https://perma.cc/F9G2-2AG3] ("If an individual suffers damage or distress because you have infringed their data protection rights . . . they are entitled to claim compensation from you. Only the courts can enforce their right to compensation."); *TAKING YOUR CASE TO COURT AND CLAIMING COMPENSATION*, INFO. COMM'R'S OFF., https://ico.org.uk/your-data-matters/data-protection-and-journalism/taking-your-case-to-court-and-claiming-compensation/ [https://perma.cc/U6LP-7Y4R] (last visited Mar. 19, 2024) ("Under data protection law, you are entitled to take your case to court to: enforce your rights under data protection law if you believe they have been breached, claim compensation for any damage caused by any organi[z]ation if they have broken data protection law, including any distress you may have suffered, or a combination of the two. The ICO cannot award compensation, even when we give our opinion that an organisation has broken data protection law.").

[196] *ENFORCEMENT OF THIS CODE*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/enforcement-of-this-code/ [https://perma.cc/37MN-QPRN] (last visited Mar. 19, 2024); Olivia Solon, *UK's Data Regulator Yet to Enforce Single Child Protection Case*, BLOOMBERG (Aug. 11, 2022), https://www.bloomberg.com/news/articles/2022-08-11/uk-s-data-regulator-yet-to-enforce-single-child-protection-case [https://perma.cc/S3TY-PY8J].

[197] *Cf.* CAL. CIV. CODE § 1798.99.31(A) (WEST 2022) *with* U.K. DESIGN CODE, *supra* note 1, at 9, 17.

[198] Joseph Duball, *California Age-Appropriate Design Code Final Passage Brings Mixed Reviews*, IAPP (Aug. 31, 2022), https://iapp.org/news/a/california-age-appropriate-design-code-final-passage-brings-mixed-reviews/ [https://perma.cc/AM6C-8HEC] ("A covered entity under the bill is defined as a business 'that provides an online service, product, or feature likely to be accessed

accessed by children" in both the U.K. Design Code and the California Design Act appear strikingly similar. However, the term "likely to be accessed" appears to possess a broader definition in the U.K. Design Code. The U.K. Design Code indicates that this phrase equates to a "*more probable than not*" standard that children will access the company's services.[199] The U.K. Design Code also expressly indicates that companies that fail to comply with the code and that have *constructive knowledge* that minors are likely to access their services can be subject to enforcement action.[200]

In contrast, the California Design Act defines the term as instances in which "it is reasonable to expect, based on" six statutory indicators, that children will access the "online service, product or feature."[201] These indicators include when "[t]he online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a *significant* number of children," among other things.[202] To meet

---

by children shall take all,' but application relies on thresholds defined under the California Privacy Rights Act."); *see also* Tyler Bridegan et al., *California Age-Appropriate Design Code Act to Impose Significant New Requirements on Businesses Providing Online Services, Products, or Features*, JD SUPRA (Sept. 1, 2022), https://www.jdsupra.com/legalnews/california-age-appropriate-design-code-8577264/ [https://perma.cc/J8W7-6R39] ("The law applies to "businesses" as defined by the California Consumer Privacy Act—a for-profit organization that does business in California and meets any of three criteria."); Arsen Kourinian et al., *What California's Child Online Safety Bill Means for Businesses*, BLOOMBERG L. (Sept. 7, 2022), https://news.bloomberglaw.com/us-law-week/what-californias-child-online-safety-bill-means-for-businesses [https://perma.cc/THH9-8UHK].

199 U.K. DESIGN CODE, *supra* note 1, at 17. The U.K. Design Code's approach has also inspired federal-level legislation. *See, e.g.*, The Protecting the Information of our Vulnerable Children and Youth Act, H.R. Res 4801, 117th Cong. (2021).

200 *See* U.K. DESIGN CODE, *supra* note 1, at 12, 18 ("[W]hether your service is likely to be accessed by children or not is likely to depend on: the nature and content of the service and whether that has particular appeal for children; and the way in which the service is accessed and any measures you put in place to prevent children gaining access.").

201 CAL. CIV. CODE § 1798.99.30(b)(4) (West 2022).

202 *Id.* § 1798.99.30(b)(4)(B) (West 2022) ("(A) The online service, product, or feature is directed to children as defined by the Children's Online Privacy Protection Act (15 U.S.C. Sec. 6501 et seq.); . . . (C) An online service, product, or feature with advertisements marketed to children. (D) An online service, product, or feature that is substantially similar or the same as an online service, product, or feature subject to subparagraph (B); (E) An online service, product, or feature that has design elements that are known to be of interest to children, including, but not limited to, games, cartoons, music, and celebrities who appeal to children. (F) A significant amount of the audience of the online service, product, or feature is determined, based on internal company research, to be children.").

this indicator, a considerable number of children must access the website. In contrast, given what appears to be a more expansive definition of the phrase "likely to be accessed by children" in the U.K. Design Code, some U.K. legal practitioners have observed that the code may be applicable, even if only a smaller number of children access a website or product.[203]

In 2022, the ICO stated that the U.K. Design Code applies to "any service being used by children living" in the United Kingdom.[204] The ICO also noted that its interpretation of the phrase "likely to be accessed by children" is in keeping with Parliament's intent "to cover services that children use in reality, but does not extend . . . to cover all services that children could possibly access."[205] The ICO notes that it took this approach in response to lessons learned from other legal frameworks internationally, which focused specifically and primarily on services designed solely for children, thereby causing regulatory gaps.[206] Rather than expressly limiting the term

---

[203] Harrison, *The UK's Age-Appropriate Design Code Comes into Force in September 2021*, *supra* note 1; Jo Joyce, *Further Protection for Children's Data – The Age Appropriate Design Code*, TAYLORWESSING (Mar. 2020), https://globaldatahub.taylorwessing.com/article/further-protection-for-childrens-data-the-age-appropriate-design-code [https://perma.cc/6X47-WWMQ] (discussing the U.K. Design Code and noting that the "ICO says that 'likely' means the possibility of access by children is 'more probable than not' but does the Code apply if it's more probable than not that an occasional child may access the service or where a very small proportion of a site's users are under [eighteen] but the site has millions of users? Even in these situations, it is likely that the site will be caught by the requirements of the [U.K.] AADC") (alteration in original); *see What Implications Will the ICO's Age Appropriate Design Code Have for Organisations?*, BATES WELLS (Nov. 30, 2021), https://bateswells.co.uk/updates/what-implications-will-the-ico-s-age-appropriate-design-code-have-for-organisations/ [https://perma.cc/5S57-P68R] (contending that the U.K. Design Code indicates that "if it subsequently becomes evident that children (even a small proportion of the overall user base) are accessing the service, the organi[z]ation will need to comply with the Code."). *But see* U.K. DESIGN CODE, *supra* note 1, at 18 ("If the nature, content or presentation of your service makes you think that children will want to use it, then you should conform to the standards in this code . . . . If you initially judge that the service is not likely to be accessed by children, but evidence later emerges that a significant number of children are in fact accessing your service, you will need to conform to the standards in this code or review your access restrictions if you do not think it is appropriate for children to use your service.").

[204] PRESS RELEASE, INFO. COMM'R'S OFF., "CHILDREN ARE BETTER PROTECTED ONLINE IN 2022 THAN THEY WERE IN 2021" - ICO MARKS ANNIVERSARY OF CHILDREN'S CODE (SEPT. 2, 2022), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/children-are-better-protected-online-in-2022-than-they-were-in-2021/ [HTTPS://PERMA.CC/HB69-PX4H].

[205] U.K. DESIGN CODE, *supra* note 1, at 17.

[206] *See id.* at 17.

"likely to be accessed by children" to a distinct list of indicators, the U.K. Design Code provides examples of instances in which the code will apply.[207] If companies believe that they are not subject to the U.K. Design Code, they are still expected to document and support the rationale behind their decision and reference any methods used to reach that conclusion and any methods used, if necessary, to prevent minors from using their services.[208] This suggests that, under the U.K. Design Code, covered entities bear the burden to prove and document why they are not subject to the code.[209]

The California Design Act's definition of the term "likely to be accessed by children" has significant similarities with standards applicable under COPPA for determining whether a service is directed towards children or whether a company has actual knowledge that it is collecting children's data. One of the six indicators listed in the California Design Act is whether the company has, under COPPA, services or products directed to minors; hence, the factors that the FTC uses to make this determination are also relevant under the California Design Act, but the application of the factors may be broader given the expanded age range in the Act.[210]

Another indicator listed to determine whether a service is "likely to be accessed by children" under the California Design Act is whether the product or service "has design elements that

---

[207] *Id*. at 17-18 ("If you have an existing service and children form a substantive and identifiable user group, the 'likely to be accessed by' definition will apply . . . [and] if your service is designed for and aimed specifically at under-[eighteen]s then the code applies. However, the provision in section 123 of the DPA is wider than this. It also applies to services that aren't specifically aimed or targeted at children but are nonetheless likely to be used by under-[eighteen]s.").

[208] *See id*. at 18.

[209] *See What Implications Will the ICO's Age Appropriate Design Code Have for Organizations*?, *supra* note 203 ("It suggests that the onus is on a website operator to clearly prove that the website does not appeal to children in order to escape the scope of the Code.").

[210] *See* CAL. CIV. CODE § 1798.99.30(b)(4)(A) (West 2022); *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FED. TRADE COMM'N (June 2017), https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business [https://perma.cc/2F8Y-EQGJ] [hereinafter *FTC Six-Step Plan*] ("The FTC looks at a variety of factors to see if a site or service is directed to children under [thirteen], including the subject matter of the site or service, visual and audio content, the use of animated characters or other child-oriented activities and incentives, the age of models, the presence of child celebrities or celebrities who appeal to kids, ads on the site or service that are directed to children, and other reliable evidence about the age of the actual or intended audience.").

are known to be of interest to children, such as games, cartoons, music and celebrities who appeal to children."[211] The presence of cartoons and celebrities who appeal to children are also factors the FTC considers in connection with making the determination of whether a site is child-directed.[212]

In applying COPPA, the FTC also considers whether there are "ads on the site or service that are directed to children."[213] Similarly, the third indicator listed in the California Design Act to determine whether children are likely to access a website is whether the online service or product has "advertisements marketed to children."[214]

The FTC's 2019 action against YouTube under COPPA suggests that actual knowledge could be obtained by a company from internal company operations and research and communications with third parties.[215] In determining whether a service is directed towards children, the FTC also considers "other reliable evidence about the age of the actual or intended audience."[216] The FTC expressly stated that "the current definition of 'website or online service directed to children' [under COPPA] already notes that [it] will consider competent and reliable empirical evidence of audience composition as part of a totality of circumstances analysis."[217] Similarly, the sixth indicator listed in the California Design Act notes that it can apply if "a significant amount of the audience of the online service, product or feature is determined, based on internal company research, to be children" and the second indicator notes that the Act can apply when "competent and reliable evidence

---

211 CAL. CIV. CODE § 1798.99.30(b)(4)(E) (West 2022). The appealable nature of the website or service to children based on its content, presentation and nature is also a relevant consideration under the U.K. Design Code, but the code makes no reference to the use of child celebrities; *see* U.K. DESIGN CODE, *supra* note 1.

212 *See FTC Six-Step Plan*, *supra* note 210.

213 *Id*.

214 CAL. CIV. CODE § 1798.99.30(b)(4)(C) (West 2022).

215 *See* Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief at 15, Fed. Trade Comm'n. v. Google LLC, No. 1:19-cv-2642 (D.D.C. Sept. 4, 2019) ("Defendants gained actual knowledge through, among other things, direct communications with channels owners, their work curating specific content for the YouTube Kids App, and their content ratings . . . In numerous instances, Defendants have knowledge of the age of the channel's target audience, either through communications with the channel owners or through its own research.").

216 *FTC Six-Step Plan*, *supra* note 210.

217 Children's Online Privacy Protection Rule, 76 FR 59804-01 (2011).

regarding audience composition" demonstrates that "a significant number of children" routinely access the service.[218]

At least five of the six indicators listed in the California Design Act to determine its applicability are somewhat similar to those used in the COPPA framework, although the California Design Act's definition does not expressly reference the company's knowledge in the same way that COPPA does.[219] Thus, the California Design Act does not appear to be a significant departure from the COPPA framework in this regard. A previous draft of the California Design Act indicated that the presence of any of the six indicators could satisfy the Act's definition of likely to be accessed, but this language

---

[218] CAL. CIV. CODE § 1798.99.30(b)(4)(F), (B) (West 2022). The ICO recommended that businesses who do not believe they are subject to the U.K. Design Code consult market research, user behavior, or other such data to determine the likelihood the code will apply. *See* U.K. DESIGN CODE, *supra* note 1, at 18.

[219] *See* 15 USC § 6502; 16 C.F.R. 312.3; Arianna Evers et al., *California's Age-Appropriate Design Code Signals Big Change for Businesses Offering Online Products and Services*, JD SUPRA (Sept. 15, 2022), https://www.jdsupra.com/legalnews/california-s-age-appropriate-design-1659690/ [https://perma.cc/BYV2-MKTH]; Kirk J. Nahra et al., *California's Age-Appropriate Design Code Signals Big Change for Businesses Offering Online Products and Services*, WILMERHALE (Sept. 14, 2022), https://www.wilmerhale.com/en/insights/blogs/WilmerHale-Privacy-and-Cybersecurity-Law/20220914-californias-age-appropriate-design-code-signals-big-change-for-businesses-offering-online-products-and-services [https://perma.cc/6E7L-P2WA]. *But see* Lisa M. Ropple et al., *California Is First State to Adopt Age-Appropriate Design Code Law Alert*, JONES DAY (Sept. 2022), https://www.jonesday.com/en/insights/2022/09/california-is-first-state-to-adopt-ageappropriate-design-code-law-alert [https://perma.cc/VBH9-U8GB] (contending that the California Design Act "applies more broadly than COPPA, where the online product, service, or feature is being accessed, or likely to be routinely accessed, by a significant number of children, without regard to the knowledge of the covered business"); James R. Carroll, *California Attorney General Announces Settlement with Sephora Under the CCPA*, SKADDEN (Sept. 2022), https://www.skadden.com/insights/publications/2022/09/privacy-cybersecurity-update [https://perma.cc/2CTW-28R3] ("[T]he standard under the Design Code Act for whether an OSPF is likely to be accessed by children is much broader than the comparable standard under COPPA, which is only applicable to operators of websites or services when such website or service is directed to children or the operator has actual knowledge that it is collecting personal information from children."). Although some practitioners suggest that the California Design Act's "likely to be accessed" indicators are broader than COPPA because they apply regardless of the company's knowledge, the COPPA factors that are similar to the California Design Act's indicators are relevant to assessing whether a site is directed towards children under COPPA. At the same time, a company's knowledge appears to be irrelevant under COPPA in making the determination of whether a site is child directed. Knowledge under COPPA is relevant to the extent that the actual knowledge standard applies.

was removed from the final version, which suggests that the Act also adopts a totality of the circumstances approach like COPPA.[220]

Perhaps one notable difference is that, although a company may not target children or market directly to children, the statutory language suggests that the company could still be subject to the California Design Act if its services are "substantially similar to" an online service that is "routinely accessed by a significant number of children."[221] Additionally, to go after YouTube, the FTC had to conduct investigations and prove that the company had actual knowledge.[222] The California Design Act's data protection impact assessment ("DPIA") provisions may make it easier to prove corporate non-compliance. It is also possible that the California Design Act may fill the regulatory gap left open by COPPA's primary coverage of data collected directly *from* covered minors.[223] In comparison to COPPA, the California Design Act appears to adopt a more expansive approach that seemingly includes personal information collected "not only *from* children, but also *about* children."[224]

---

[220] *See* Assembly B. 2273, 2021-22 Gen. Assembly, Reg. Sess. § 1(a)(1) (Cal. 2022) (to view the earlier version, locate the bill on the official "California Legislative Information" website, select "Compare Versions," and using the dropdown menu that allows for a comparison against the current September 15, 2022 version, select "8/11/2022 – Amended Senate" and then click "Compare Versions." Notably, under section § 1798.99.30. (b)(4), the language "any of" will appear in red and will have a line running through it, and "indicators" will replace the word "factors."). *Cf. with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (July 22, 2020), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions [https://perma.cc/EZV7-JJ52] [hereinafter COPPA FAQs].

[221] CAL. CIV. CODE § 1798.99.30(b)(4) (West 2022).

[222] *See* Protecting Kids Online: Internet Privacy and Manipulative Marketing: Hearing Before the Subcomm. on Consumer Prot., Prod. Safety, and Data Sec., 117th Cong. (2021) (statement of Angela J. Campbell, Chair, Campaign for a Commercial-Free Childhood).

[223] *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 798 (8th ed. 2023) ("COPPA does not apply to information collected from adults about children under 13; it only applies to personal data collected from children themselves.").

[224] CHLOE ALTIERI & BAILEY SANCHEZ, FUTURE OF PRIVACY FORUM, POLICY BRIEF: AN ANALYSIS OF THE CALIFORNIA AGE APPROPRIATE DESIGN CODE 6 (2022), https://fpf.org/wp-content/uploads/2022/10/FPF-Policy-Brief-California-Age-Approp-Design-Code-R2.pdf [https://perma.cc/E22S-HLR6] ("COPPA regulates how businesses may collect and user personal information obtained *from* children. The California AADC seems to take a broader approach that may include information not only *from* children, but also *about* children such as metadata or augmented data."). To the extent that the California Design Act, relies on the CCPA's definition of personal information, the statute could provide protections

There is also a notable difference between COPPA and the California Design Act's approach to connected devices. In some instances, COPPA can apply to IoT devices. For example, connected IoT toys are likely to be viewed as services and products that are directed towards children and, if so, are subject to COPPA.[225] The similarities between COPPA's scope and the California Design's Act scope discussed earlier would suggest that connected toys are covered by the California Design Act. However, the California Design Act excludes "the delivery or use of a physical product" from the definition of the term "online service, product or feature," which itself appears in the definition of the term "likely to be accessed by children."[226] It is not entirely clear whether this exemption for physical products will exclude all aspects of IoT devices and associated online services or only the delivery and use of the hardware and physical components of such products. IoT devices are often associated with various online services and software, such as mobile apps, that are connected to physical device functionality. If the terms "delivery or use" are interpreted broadly, all aspects of IoT toys and devices, including purely online components, could be excluded from coverage. If such an interpretation is adopted, the California Design Act is unlikely to remedy concerns discussed in Part I that are associated with IoT devices. This might be an area that the

---

for broad categories of children's personal information as defined under the CCPA. Nerissa Coyle McGinn, *California: COPPA v. CAADC - Strength Lies in Knowing The Differences*, (Apr. 2023) https://www.dataguidance.com/opinion/california-coppa-v-caadc-strength-lies-knowing [https://perma.cc/TS3C-FX29] ("Personal information under the CAADC uses the same definition in Section 1798.140 of the California Privacy Rights Act of 2020. This definition arguably is broader than COPPA . . . . COPPA is limited to information collected from children online. The CAADC does not have this limitation. It can include either information collected from parents . . . ."); *see* CAL. CIV. CODE § 1798.140(v)("(1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.").

225 *See* COPPA FAQs, *supra* note 220 (The COPPA "Rule applies to operators of commercial websites and online services (including mobile apps and IoT devices, such as smart toys) directed to children under 13 that collect, use, or disclose personal information from children, or on whose behalf such information is collected or maintained (such as when personal information is collected by an ad network to serve targeted advertising)."); Stacey Gray, *Federal Trade Commission: COPPA Applies to Connected Toys*, FUTURE PRIV. F. (June 26, 2017), https://fpf.org/blog/federal-trade-commission-coppa-applies-connected-toys/ [https://perma.cc/9KXC-LJLZ].

226 CAL. CIV. CODE § 1798.99.30(b)(4) (West 2022).

California attorney general may shed light on via regulation in accordance with statutory authorization.[227]

In contrast, the U.K. Design Code clearly notes that it applies to connected devices and toys, and it describes these objects as "physical products which are supported by functionality provided through an internet connection."[228] Connected toys and devices are included in the U.K. Design Code as one of the fifteen standards established under the code. The express lack of a reference to connected toys in the California Design Act while including references to other standards from the U.K. Design Code suggests an intent to exclude, at the very least, the physical components of such devices. To the extent that connected toys and devices are excluded from the California Design Act, it is also unlikely that the Act would apply to IoT devices geared towards adults, even though data about children could be collected through children's use of such products and these products may be "routinely accessed by a significant number of children."[229] The difference in the approach between the U.K. Design Code and the California Design Act could be due to COPPA's pre-existing regulation of IoT connected toys, COPPA's preemption of inconsistent state laws, or perhaps legislative attempts to accommodate industry objections to the breadth of the statute.

iv. Age Verification Versus Age Estimation

The U.K. Design Code and the California Design Act appear to adopt somewhat different approaches on the topic of age assurance, which experts have defined to include both age estimation and age verification techniques.[230] The California Design Act requires firms to "*estimate* the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business or apply the privacy and data protections

---

227 *See* CAL CIV CODE § 1798.99.35(e) (West 2022)

228 U.K. DESIGN CODE, *supra* note 1, at 78.

229 CAL. CIV. CODE § 1798.99.30(b)(4)(B) (West 2022).

230 The term age assurance is "an umbrella term for both age verification and age estimation solutions. The word 'assurance' refers to the varying levels of certainty that different solutions offer in establishing an age or age range." 5 RIGHTS. FOUND., BUT HOW DO THEY KNOW IT IS A CHILD? 6 (Oct. 2021), https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf [https://perma.cc/6CTA-57SK].

afforded to children to all consumers."[231] The U.K. Design Code, by comparison, requires entities to either apply the code's standards to all users or "*establish* age with a level of certainty that is appropriate to the risks" related to data processing.[232] The COPPA rule does not require websites "to ask the age of visitors."[233] However, under COPPA, companies whose services do not target children as their main users but whose services qualify as being directed to children under relevant COPPA factors, can elect to apply COPPA protections only to customers under age thirteen, but if the company chooses that option, it "must not collect personal information from any users without first collecting age information."[234]

Although the U.K. Design Code indicates that it does not require companies to use a specific method to determine age or establish age with a specific level of certainty, the U.K. Design Code uses the term "establish" (and in some cases "estimate") while the California Design Act uses the term "estimate."[235] This difference in language may be an important one as it suggests that, under the California Design Act, an approximation of age that sorts children into developmental age ranges referenced in the legislative findings and declarations portion of the bill enacting the statute, rather than an exact determination, would be sufficient. This difference perhaps reflects an attempt by the California legislature to clearly avoid mandating or incentivizing the use of hard identifiers and to encourage companies to use existing data to estimate age instead.

---

231 CAL. CIV. CODE § 1798.99.31(b)(8) (West 2022).

232 U.K. DESIGN CODE, *supra* note 1, at 7 (The U.K. Design Code requires covered entities to "[e]ither establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead."); *see* INFORMATION COMM'R'S OFF., AGE ASSURANCE FOR CHILDREN'S CODE (2021), https://ico.org.uk/media/4018659/age-assurance-opinion-202110.pdf [https://perma.cc/W2N7-NN96] (providing additional guidance on age assurance under the U.K. Design Code); *see also* Camille Carlton, *Why The California Age Appropriate Design Code Is Groundbreaking*, CTR. FOR HUMANE TECH. (Sept. 29, 2022), https://www.humanetech.com/insights/why-the-california-age-appropriate-design-code-is-groundbreaking [https://perma.cc/DB8K-5MM8] ("The CA Kids Code does not require age verification nor is it a likely outcome of the bill as there has been no age verification scheme in the UK following the UK's AADC.").

233 COPPA FAQs, *supra* note 220.

234 *FTC Six-Step Plan*, *supra* note 210.

235 UK DESIGN CODE, *supra* note 1, at 33-34 ("It may be possible to make an estimate of a user's age by using artificial intelligence to analyse the way in which the user interacts with your service. Similarly, you could use this type of profiling to check that the way a user interacts with your service is consistent with their self-declared age.")

There are both practical and potential First Amendment concerns with vague age verification mandates. Many age verification techniques require users to provide government IDs, credit cards, or other data to verify the user's age, and although "all of these methods have varying success . . . none have mastered a combination of privacy, efficiency and affordability yet."[236] In *Reno v. ACLU*, the Supreme Court found that the provisions of the Communication Decency Act ("CDA") on "indecent transmission" and "patently offensive display," which were applicable to children under the age of eighteen and which included a defense if actors implemented age verification processes that restricted children's access "by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number," violated the First Amendment. [237] The Court reasoned that several provisions

---

[236] Jackie Snow, *Why Age Verification Is So Difficult for Websites*, WALL ST. J. (Feb. 27, 2022), https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728 [https://perma.cc/D9TL-VG6N].

[237] Reno v. ACLU, 521 U.S. 844, 845 (1997) ("[The CDA of 1996] criminalizes the 'knowing' transmission of 'obscene or indecent' messages to any recipient under 18 years of age . . . prohibits the 'knowin[g]' sending or displaying to a person under 18 of any message 'that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs.' Affirmative defenses are provided for those who take 'good faith, . . . effective . . . actions' to restrict access by minors to the prohibited communications, . . . and those who restrict such access by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number . . . ."); *see also* 47 U.S.C. § 223 (2018). After *Reno*, Congress passed the Child Online Protection Act of 1998, which also contained age verification provisions associated with sexually explicit materials, but that law was also struck down for violating the First Amendment. Emily R. Purdy, *Child Online Protection Act of 1998*, FREE SPEECH CTR. (Aug. 8, 2023), https://www.mtsu.edu/first-amendment/article/1066/child-online-protection-act-of-1998 [https://perma.cc/P3BN-EFS3]; Jeffery D. Neuburger, *U.S. Supreme Court (Finally) Kills Online Age Verification Law*, MEDIASHIFT (Jan. 29, 2009), http://mediashift.org/2009/01/u-s-supreme-court-finally-kills-online-age-verification-law029/amp/ [https://perma.cc/U6TK-AQ9L]; *see also* ACLU v. Gonzalez, 478 F. Supp. 2d 775 (E.D. Pa. 2007) *aff'd*, 534 F.3d 181 (3d Cir. 2008), *cert. denied*, 129 S. Ct. 1032 (2009) ("From the weight of the evidence, I find that there is no evidence of age verification services or products available on the market to owners of Web sites that actually reliably establish or verify the age of Internet users."). In contrast, the California Design Act requires age estimation rather than age verification. It is unclear whether this difference may be helpful in negating First Amendment challenges considering *Reno*. *See* Mike Masnick, *The Supreme Court Already Explained Why California's Age Appropriate Design Code Is Unconstitutional*, TECHDIRT (Sept. 2, 2022), https://www.techdirt.com/2022/09/02/the-supreme-court-already-explained-why-californias-age-appropriate-design-code-is-unconstitutional/ [https://perma.cc/LA6S-4WN9]; Joseph Duball, *California Age-Appropriate Design Code Final Passage Brings Mixed Reviews*, IAPP (Aug. 31, 2022),

contained in the CDA were vague and could have a chilling effect on speech because, "in order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another."[238] The Court seemingly called into question the validity of laws that chill speech based on the likelihood that children may access speech intended for adults, particularly given difficulties with age verification processes.[239] It is notable that the California Design Act does not contain a clear definition of the term "reasonable level of certainty appropriate to the risks."

While age verification requires the use of verified sources of identification that provide a strong degree of reliability regarding a user's age and often reveals identity, age estimation involves processes "that establish that a user is *likely* to be of a certain age, fall within an age range, or is over or under a certain age."[240] The U.K. Design Code recognizes the tension between age assurance and data

---

https://iapp.org/news/a/california-age-appropriate-design-code-final-passage-brings-mixed-reviews/ [https://perma.cc/LRG3-T4GZ]; Eric Goldman, *Will California Eliminate Anonymous Web Browsing?*, TECH. & MKTG. L. BLOG (June 27, 2022), https://blog.ericgoldman.org/archives/2022/06/will-california-eliminate-anonymous-web-browsing-comments-on-ca-ab-2273-the-age-appropriate-design-code-act.htm [https://perma.cc/6D7C-8M84].

238 *Reno*, 521 U.S. at 874 ("That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.").

239 *See id*. at 876-78 ("The findings of the District Court make clear that this premise is untenable. Given the size of the potential audience for most messages, in the absence of a viable age verification process, the sender must be charged with knowing that one or more minors will likely view it. Knowledge that, for instance, one or more members of a 100-person chat group will be a minor—and therefore that it would be a crime to send the group an indecent message—would surely burden communication among adults."); *see also* Complaint for Declaratory Judgment and Injunctive Relief, Netchoice LLC v. Bonta, 5:22-cv-8861 (N.D. Cal. Dec. 14, 2022).

240 5 RTS. FOUND., *supra* note 230, at 6 ("Age estimation methods include automated analysis of behavioural and environmental data; comparing the way a user interacts with a device or with other users of the same age; metrics derived from motion analysis; or testing the user's capacity or knowledge . . . data used to assure age can also be derived from contextual information about a person's use of a service, for example the type of content they frequently interact with, . . . the times and frequency they are 'active' . . . or they can be put into an age range by their ability to complete a given task or their use of language . . . . [D]ata relating to physical characteristics, such as height and gate are commonly collected by devices such as phones or wearable fitness trackers, and can indicate the likely age of users.").

minimization but notes that "age assurance and the GDPR are compatible if privacy by design solutions are used."[241]

With respect to concerns about anonymity, to satisfy age estimation or age verification requirements, companies may need to collect significant amounts of data, including potentially biometric identifiers. Additional instances of data collection could contribute to growing concerns about children's anonymity online and negatively impact the functionality of services and products accessed by adults.[242] While age verification technology has advanced since the 1990s, age verification remains a challenging issue. Additionally, at least one scholar has suggested that U.K. regulators are likely to accept firms "good-faith efforts" to comply with the U.K. Design Code, even if full compliance is not achieved, which is in contrast to the approach often taken in the United States.[243]

Newer developments, such as age tokens through QR codes, may help to protect users anonymity and minimize data collection by multiple companies while verifying or estimating users age.[244] Additionally, nascent developments in artificial intelligence could allow companies to identify or estimate users age without requiring users to provide additional sensitive data.[245] The U.K. Design Code acknowledges these developments.[246] In 2021, Meta announced plans to use artificial intelligence to infer users' age by analyzing multiple signals including self-reported age, age referenced in birthday messages and age listed in other associated "accounts, such

---

241 U.K. DESIGN CODE, *supra* note 1, at 35.

242 *See* Goldman, *supra* note 237.

243 Eric Goldman, *An Interview Regarding AB 2273/California Age-Appropriate Design Code*, TECH. & MKTG. L. BLOG (Sept. 7, 2022), https://blog.ericgoldman.org/archives/2022/09/an-interview-regarding-ab-2273-the-california-age-appropriate-design-code-aadc.htm [https://perma.cc/V3BF-GSDH].

244 *See* Snow, *supra* note 236. Indeed, an age token "contains only information relating to the specific age or age range of a user. This allows the service to establish if a user meets age requirements without collecting other personal information." 5 RTS. FOUND., *supra* note 230, at 38. Additionally, age tokens also "minimise the amount of data that is shared with services and could be used more widely if the technology was readily available to a greater number of trusted institutions." *Id*. at 39.

245 *See* Snow, *supra* note 236 ("Some of the biggest online companies are turning to artificial intelligence to estimate age without requiring additional data.").

246 *See* U.K. DESIGN CODE, *supra* note 1, at 34.

as Instagram."[247] Companies have long used various techniques to estimate the age of users in connection with targeted advertising.[248]

The California Design Act attempts to address concerns about anonymity and the misuse of age estimation data by prohibiting firms from using any collected age estimation data for other purposes.[249] Covered entities are also prohibited from retaining age estimation data "longer than necessary to estimate age."[250] How effective these restrictions will be remains to be seen and will likely depend on the state attorney general's enforcement efforts. Additionally, even if this restriction proves to be effective in preventing subsequent disclosures and uses of age estimation data, it may not fully address issues related to the initial data collection or the data analysis that may be necessary to estimate age.

Lastly, recall that some states, including Illinois, have proposed laws that are similar to the California Design Act.[251] As is the case with other privacy laws adopted in California, the California Design Act may also influence companies' practices in other states. To the extent that biometric identifiers assist in age estimation or assurance efforts, it is unclear whether state laws encouraging age assurance will be incompatible with existing state biometric data laws, including provisions mandating consent for the collection of

---

247 Snow, *supra* note 236 ("Meta Platforms Inc. outlined its use of AI to continually cross-check accounts on its Facebook and Instagram sites for information that can belie or confirm a user's stated age. For instance, if someone lists their age as 18 but has a friend sending them a 'Happy Quinceañera'—15th birthday—message, that could be a red flag."); 5 RTS. FOUND., *supra* note 230, at 32 (Meta "will use multiple signals such as the age of users indicated in birthday messages and comparing the self-declared age of users with the age indicated in linked accounts, such as Instagram.").

248 Hany Farid, *Don't Let Fearmongering Derail a New Law that Has Real Teeth to Protect Kids' Privacy*, GIZMODO (Sept. 8, 2022), https://gizmodo.com/age-appropriate-design-code-california-kids-privacy-1849508115 [https://perma.cc/B5BV-CMVH] ("Age estimation can be done in a multitude of ways that are not invasive. In fact, businesses have been using age estimation for years – not to keep children safe – but rather for targeted marketing.").

249 *See* CAL. CIV. CODE § 1798.99.31(b)(8) (West 2022) (A business subject to this law may not "[u]se any personal information collected to estimate age or age range for any other purpose or retain that personal information longer than necessary to estimate age. Age assurance shall be proportionate to the risks and data practice of an online service, product, or feature.").

250 *Id.*

251 *See* Illinois Age-Appropriate Design Code Act., 2023 Legis. Bill Hist. IL S.B. 1126 ("A business that provides an online service, product, or feature likely to be accessed by children shall not take any of the following actions: . . . Use any personal information collected to estimate age or age range for any other purpose or retain that personal information longer than necessary to estimate age.").

biometric identifiers and authorizing the retention of biometric identifiers.[252] Illinois' BIPA permits the retention of biometric identifiers until the initial purpose for collecting the data is over or "within three years of the" customers' last interaction with the covered entity, whichever is earlier.[253] Texas' biometric data statute provides a one year outside date for the destruction of biometric identifiers.[254]

b. Relatively Similar Provisions

The U.K. Design Code consists of "a set of [fifteen] flexible standards" intended to encourage built-in privacy protections for children in online services and products "to allow children to [safely] explore, learn and play online."[255] The California Design Act borrows and, in some cases, adjusts some of these standards. Thus, despite important differences highlighted earlier, the California Design Act and the U.K. Design Code are relatively similar in several ways. Examples of relative similarities include the definition of a child, the best interest of the child standard, the imposition of privacy by default and design obligations,

---

[252] *See* Eric Goldman, *Do Mandatory Age Verification Laws Conflict with Biometric Privacy Laws? – Kuklinski v. Binance*, TECH. & MKTG. L. BLOG (Apr. 8, 2023), https://blog.ericgoldman.org/archives/2023/04/do-mandatory-age-verification-laws-conflict-with-biometric-privacy-laws-kuklinski-v-binance.htm [https://perma.cc/RU7N-44W7] (noting that "face scanning seemingly directly conflict[s] with biometric privacy laws, such as Illinois' BIPA [and] . . . [a]nother possible tension is whether the business can retain face scans, even with BIPA consent, in order to show that each user was authenticated if challenged in the future, or if the face scans need to be deleted immediately, regardless of consent, to comply with privacy concerns in the age verification law.").

[253] 740 ILL. COMP. STAT. ANN. 14/15 ("A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first."). California regulates biometric identifiers as sensitive information under the CCPA. *See* CAL CIV CODE § 1798.140 (West 2023).

[254] *See* TEX. BUS. & COM. CODE ANN. § 503.001(c)(3) (a covered entity in possession of biometric identifiers "shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires, except as provided by Subsection (c-1).").

[255] U.K. DESIGN CODE, *supra* note 1, at 4.

restrictions on data monetizations, restrictions on detrimental conduct, age transparency requirements and DPIA obligations. The California Design Act's incorporation of several of the U.K. Design Code's standards, such as DPIA obligations and restrictions on tracking children without their knowledge, may allow it to improve privacy protections in some contexts.[256]

Additionally, although there are instances in which some of the California Design Act's provisions share similarities with COPPA's framework, such as the likely to be accessed by children indicators, there are some differences, some of which were discussed earlier. One notable additional difference discussed in this section is the California Design Act's expanded age range. Further, the U.K. Design Code and the California Design Act represent a departure from COPPA's approach of treating parents as the main gatekeepers of children's privacy given both frameworks' emphasis on corporate actors considering the best interests of children.[257]

i. Who Is a Child?

The U.K. Design Code and the California Design Act both define a child as an individual under the age of eighteen.[258] The California Design Act's incorporation of a broad definition of the term child is notable given COPPA's limited under thirteen age range. Unlike COPPA, the California Design Act provides special protections for children ages thirteen through seventeen. The California Design Act's coverage of older children could fill the regulatory gap left open by COPPA's limited age range. Similarly,

---

256 *See* Grande, *Calif.'s Novel Privacy Moves May Dim Federal Law's Chances*, *supra* note 181; Pixalate, *COPPA vs the California Age-Appropriate Design Code*, PIXALATE BLOG (Sept. 21, 2022), https://www.pixalate.com/blog/coppa-vs-caadc?hs_amp=true [https://perma.cc/F5SV-SXKP].

257 *See* Ariel Fox Johnson, *Reconciling the Age Appropriate Design Code with COPPA*, IAPP (Feb. 23, 2021), https://iapp.org/news/a/reconciling-the-age-appropriate-design-code-with-coppa/ [https://perma.cc/D8C8-3MWG]; Alexander Brown et al., *ICO's Age Appropriate Design Code Comes into Force*, SIMMONS & SIMMONS (Oct. 27, 2020), https://www.simmons-simmons.com/en/publications/ckgs2ty6aadwl0a43e3avb7r3/ico-s-age-appropriate-design-code-comes-into-force [https://perma.cc/K34S-5CEC].

258 *Cf.* CAL. CIV. CODE § 1798.99.30(b)(1) (West 2022) *with* U.K. DESIGN CODE, *supra* note 1, at 17. The California Design Act is not the first California law to provide privacy protections to children through the age of eighteen. *See* CAL. BUS. & PROF. CODE § 22580 (West 2019).

the UNCRC also defines a child as a person under the age of eighteen.[259]

Like the ICO's forward in the U.K. Design Code, the uncodified preamble of the bill enacting the California Design Act notes that the UNCRC "recognizes that children need special safeguards and care in all aspect of their lives."[260] Additionally, the legislative findings and declarations of the bill on which the California Design Act is based divides children into the same developmental age ranges established under the U.K. Design Code.[261]

ii. Best Interests of the Child

Both the U.K. Design Code and the California Design Act emphasize that covered entities should consider the best interests of children when designing and developing their products and services. This language features prominently in several of the U.K. Design Code's standards and the California Design Act's codified requirements and legislative findings and declarations.[262] The California Design

---

[259] *See* Convention on the Rights of the Child, Sept. 2, 1990, 1577 U.N.T.S. 27531, pt. 1, art. 1.

[260] *Cf.* Assembly B. 2273, 2021-22 Gen. Assembly, Reg. Sess. § 1(a)(1) (Cal. 2022) (enacted) ("The Legislature finds and declares that . . . (1) The United Nations Convention on the Rights of the Child recognizes that children need special safeguards and care in all aspects of their lives.") *with* U.K. DESIGN CODE, *supra* note 1, at 3 ("This code will lead to changes in practices that other countries are considering too. It is rooted in the United Nations Convention on the Rights of the Child . . . that recogni[z]es the special safeguards children need in all aspects of their life. Data protection law at the European level reflects this and provides its own additional safeguards for children.").

[261] *Cf.* Cal. Assembly B. § 1(a)(5) (describing "0-5" as "pre-literate and early literacy," "6-9" as "core primary school years," "10-12" as "transition years," "13-15" as "early teens," "16-17" as "approaching adulthood") *with* U.K. DESIGN CODE, *supra* note 1, at 32 (containing the same age groups).

[262] *See* Assembly B. 2273, 2021-22 Gen. Assembly, Reg. Sess. (Cal. 2022) (enacted). At least two of the California Design Act's references to the best interest of the child appear to be located in "the non-binding legislative findings," including the statement that businesses "should consider the best interests of children when designing" and developing products that prioritize the "privacy, safety, and well-being of children over commercial interests." ALTIERI & SANCHEZ, *supra* note 224, at 3. However, the obligation in the California Design Act to use high privacy settings by default and the statute's restrictions on data monetizations, data collection, and data uses and profiling incorporate the best interest of the child standard. *See* CAL. CIV. CODE § 1798.99.31(a)(6) (West 2022). The U.K. Design Code notes that the best

Act's inclusion of the best interest of the child standard could also be viewed as an attempt to incorporate some aspects of a fiduciary duty of loyalty into privacy legislation. Some scholars have advocated for the imposition of a duty of loyalty in the privacy law context that adopts a "best interests" approach.[263]

The potential efficacy of a best interest of the child standard in the privacy and data security context may be critiqued on several grounds. One is that the standard is vague, rendering it difficult to apply in the online context.[264] Continuing that line of argument, vague legal standards may grant too much power to "compliance professionals" to apply and define the standard in practice.[265] As a result, there may be a significant risk of legal endogeneity in which meager signs of compliance, such as companies hiring data protection officers, give the illusion of concrete privacy protection and compliance.[266] In practice, companies and their data compliance

---

interest of the child standard is rooted in the UNCRC. *See* U.K. DESIGN CODE, *supra* note 1, at 24. In determining whether a covered entity is acting in the best interest of children, the entity must consider the "rights they hold under the United Nations Convention on the Rights of the Child." *BEST INTEREST OF THE CHILD SELF-ASSESSMENT*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/childrens-code-hub/best-interests-of-the-child-self-assessment/ [https://perma.cc/83NB-GXLQ] (last visited Mar. 18, 2024). In particular, "you should consider how, in your use of personal data, you can: keep them safe from exploitation risks, including the risks of commercial or sexual exploitation and sexual abuse; protect and support their health and wellbeing; protect and support their physical, psychological and emotional development; protect and support their need to develop their own views and identity; protect and support their right to freedom of association and play." U.K. DESIGN CODE, *supra* note 1, at 25.

263 Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 961 (2021). Professors Richards and Hartzog first discuss various forms of the duty of loyalty in U.S. law. *See id*. at 968. They then contend that, "given the nature of the digital landscape, the relative unsophistication of most digital consumers, and the technical, legal, and economic power differentials between consumers and platforms," that "the 'best interests' form of loyalty is best suited to protect digital consumers. The best-interests approach would have the additional benefit of ridding trusting consumers of the burdens of privacy self-management and other 'privacy work.'" *Id.*

264 Proposals for a duty of loyalty in the online context have also faced similar critiques. *See, e.g.*, James Grimmelmann, *When All You Have Is a Fiduciary*, L & POL. ECON. PROJECT (May 30, 2019), https://lpeproject.org/blog/when-all-you-have-is-a-fiduciary [https://perma.cc/69UY-PD8A] (critiquing a duty of loyalty and contending that the "difficulty is that the problem of making [online] recommendations is so complex that it is hard to flesh out the contours of disloyalty in an administrable way").

265 Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 31 (2020).

266 *See id.*

professionals may frequently frame legal obligations "in accordance with managerial values like operational efficiency and reducing corporate risk rather than the substantive goals the law is meant to achieve, like consumer protection."[267] If companies are given too much power to define and determine how to comply with the best-interest-of-the-child standard, they may inevitably choose an approach that most benefits their bottom line, while using basic symbols of privacy compliance. These symbols of compliance could eventually be viewed as best practices and influence policymakers and lawmakers' interpretation of compliance with applicable legal requirements.[268] Today, companies often craft their privacy policies to imply that they are acting in consumers' best interest by, for instance, collecting and using data to provide services to consumers. One might posit that, if left unchecked, companies will continue to do so, even if a best-interest-of-the-child standard is adopted.

One response to this critique is that vague standards promote flexibility, which, in turn, enables laws to adapt more readily to new societal and technological changes. Seemingly vague standards contained in the GDPR are working to some extent in Europe, and are even featured in American family law, which uses the best interest of the child standard. In the latter setting, some state legislatures, to combat the vagueness concerns, have required courts to not only use specific factors in applying the standard, but also to expressly address and provide an analysis of the factors in their decisions.[269] Additionally, the California Design Act attempts to alleviate some of the foregoing concerns by noting in the legislative findings and declaration section that in the event of a conflict between the best interests of children and firms' commercial interests, firms should "prioritize the privacy, safety and well-being of children over commercial interests."[270] Somewhat similarly, the

---

267 *Id*. at 776.

268 *See id.* at 777 (discussing legal endogeneity and contending that "some of privacy law's most important tools [such as] . . . consent requirements, and FTC consent decrees—are so unclear that professionals on the ground have wide latitude to frame the law's requirements, kicking endogeneity into high gear").

269 *See, e.g.*, Cal Fam Code § 3011 (West 2023); § 452.375 R.S.Mo. (West 2023); Powell v. Ayars, 792 So. 2d 240, 244 (Miss. 2001); Myers v. Myers, 270 So. 3d 1060, 1064 (Ala. Civ. App. 2018) (citing *Powell* and stating that "the chancellor is required to address each [best interests of the child] factor that applies to the case before him"). *See generally* Carl Funderburk, *Best Interest of the Child Should Not Be an Ambiguous Term*, 33 CHILD. LEGAL RTS. J. 229 (2013) (making the argument that term should not be ambiguous).

270 CAL. CIV. CODE § 1798.99.29(b) (West 2022).

U.K. Design Code indicates that covered entities should "account for the best interests of the child as a primary consideration where any conflict [between a firms' commercial interests and children's interests] arise."[271]

With respect to statutory ambiguities and the California Design Act, recall that in the uncodified preamble, the California legislature expressly declared its intent to encourage businesses to rely on guidance issued by the U.K. ICO under the U.K. Design Code, established the CDWG to investigate and report on best practices for implementation of the Act, and empowered the California attorney general to adopt regulations to clarify statutory requirements.[272] The U.K. ICO already issued relevant guidance to companies on how they can satisfy the best interest of the child standard by offering a best interest of the child self-assessment tool and additional design guidance on practical implementation of the code.[273]

Another possible critique of the best interests of the child approach is that it conflicts with companies' duties to their shareholders. Proposals to implement an information fiduciary approach in the privacy law context that incorporates duties of care and loyalty have also faced similar critiques.[274] However, there are

---

[271] U.K. DESIGN CODE, *supra* note 1, at 26.

[272] *See* Assembly B. 2273, 2021-22 Gen. Assembly, Reg. Sess. § 1(d)-(f) (Cal. 2022) (enacted).

[273] *See BEST INTEREST OF THE CHILD SELF-ASSESSMENT*, *supra* note 262; Georgina Bourke & Ahmed Razek, INFORMATION COMM'R'S OFF., CHILDREN'S CODE DESIGN GUIDANCE 4-34 (2022), https://ico.org.uk/media/for-organisations/documents/4019528/childrens-code-ebook-2022.pdf [https://perma.cc/DUY8-2C7Z].

[274] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 102-04 (N.Y.U. Press 2004) ("I posit that the law should hold that companies collecting and using our personal information stand in a fiduciary relationship with us."); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016) (discussing information fiduciaries); Jane R. Bambauer, *The Relationships Between Speech and Conduct*, 49 U.C. DAVIS L. REV. 1941, 1944 (2016); Woodrow Hartzog & Neil Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. 356, 356 (2022); Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 498-502 (2019); Richards & Hartzog, *supra* note 263, at 966 ("Under our approach, loyalty would manifest itself primarily as a prohibition on designing digital tools and processing data in a way that conflicts with a trusting party's best interests. Data collectors bound by such a duty of loyalty would be obligated to act in the best interests of the people exposing their data and engaging in online experiences, but only to the extent of their exposure."); Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ [https://perma.cc/WPQ9-2LKN].

other sources of law, such as consumer protection laws, that could arguably conflict with corporate directors' duties to shareholders.[275] One might posit that managements' compliance with established legal rules and requirements in conducting the firms' business is, to some extent, separate from a director's duty to shareholders.[276]

Despite the foregoing criticisms, an emphasis on considering the best interests of the child moves the law away from an overreliance on notice and choice (parental or child consent) and privacy self-management, and, instead, places a greater burden on businesses to protect children's data and consider children's well-being when developing and designing their services and products. This approach could aid in correcting existing legal frameworks' overreliance on parental notice and choice and, at a minimum, provide protections to children not within COPPA's framework solely because of their age. Additionally, a best interest of the child approach could also help address civil liberties and monetization issues by potentially making companies more inclined to consider these concerns when designing products and implementing their business models. However, recall the seeming exclusion of IoT products from the statute's coverage.

The best interest approach may also facilitate the development of online services that are more likely to be protective of children's privacy. Recall the studies discussed in Part I indicating that children in lower-income and lower-educated households may be more at risk for privacy invasions because of their parents' choices and limited privacy related knowledge. If services that children are likely to access are more privacy protective to begin with, then differences associated with children's privacy resulting from parents' income and educational status could be minimized. Covered entities can be encouraged to consider children's best interest when designing and developing their services regardless of

---

[275] Balkin notes that "consumer protection law, environmental law, or antitrust law are logically incoherent and unenforceable because they conflict with management's duty to maximize shareholder value." Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. 11, 23 (2020).

[276] Balkin also observes that "management's fiduciary obligations to shareholders assume that the corporation will attempt to comply with the legal duties owed to those affected by the corporation's business practices, even if this reduces shareholder value." *Id*. He also notes that, indeed, "management's duty of loyalty to shareholders requires directors to make good faith efforts to ensure that the corporation complies with all regulatory laws that apply to its operations." *Id*. n.55.

the privacy choices parents or children make after the services are made available to the public.

iii. Privacy by Design

The U.K. Design Code and the California Design Act both incorporate various aspects of a privacy by design approach, such as default privacy settings, DPIA requirements, "respect for user privacy" and "embedding privacy into design."[277] The U.K. Design Code expressly references the GDPR's privacy by design and default obligations in connection with the standards established under the code.[278] Incorporation of the best interest of the child standard is perhaps loosely connected to a core aspect of privacy by design—"respect for user privacy," which requires "architects and operators to keep the interests of the individual uppermost."[279] Obligations to configure settings to ensure a high level of privacy, to conduct

---

[277] Assembly B. 2273, 2021-22 Gen. Assembly, Reg. Sess. § 1 (Cal. 2022) (enacted). ("Online services, products, or features that are likely to be accessed by children should offer strong privacy protections by design and by default"). The California Design Act requires businesses that provide products or services that children will likely access to, among other things, "[c]onfigure all default privacy settings provided to children by the online service, product, or feature to settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children." CAL. CIV. CODE § 1798.99.31(a)(6) (West 2022). By comparison, the U.K. DESIGN CODE states that settings "must be 'high privacy' by default" (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child." U.K. DESIGN CODE, *supra* note 1, at 50. For more on why DPIAs matter for data privacy, *see* INFO. COMM'R OFF., DATA PROTECTION BY DESIGN AND DEFAULT 31 (2022), https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance-0-0.pdf [https://perma.cc/75S2-85VV] ("DPIAs are an integral part of data protection by design and by default. For example, they can determine the type of technical and organi[z]ational measures you need in order to ensure your processing complies with the data protection principle."); *see* Lee A. Bygrave, *Data Protection by Design and By Default*, *in* THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 571, 571-79 (Christopher Kuner et al. eds., Oxford Univ. Press 2020) (discussing the GDPR's privacy by design obligations).

[278] *See* U.K. DESIGN CODE, *supra* note 1, at 11, 50, 54.

[279] ANN CAVOUKIAN, THE 7 FOUNDATIONAL PRINCIPLES 5 (2011), https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf [https://perma.cc/JN6N-H22K] (listing the seven foundational principles of privacy by design). Similarly, some view the GDPR's privacy by design obligations as creating a duty on controllers to implement technological and organizational measures "to ensure protection of data subjects' rights." Bygrave, *supra* note 277, at 576.

DPIAs before a product's release, and to maintain and address risks identified in same all reflect the incorporation of another important privacy by design principle—a proactive rather than remedial approach; they also reflect a commitment "to set and enforce high standards of privacy."[280] We will come back to the topic of DPIAs in more detail below.

Under both regimes, privacy settings for children should, by default, provide a strong level of privacy unless the company can "demonstrate a compelling reason that a different setting is in the best interests of children."[281] The term "compelling reason" is not defined in the California Design Act, but the U.K. Design Code provides guidance with respect to the use of this term in some contexts.[282] Examples of a compelling reason to share child data include fraud protection, child abuse and exploitation.[283] The U.K. Design Code's and the California Design Act's approach can be viewed as an attempt to operationalize and reinvigorate privacy by design. The FTC also recommended privacy by design.[284]

Admittedly, privacy by design has too received criticism for vagueness, although scholars have varying views on privacy by design requirements.[285] However, the European Data Protection Board has issued guidance and data protection authorities'

---

[280] CAVOUKIAN, *supra* note 279, at 2; *see also* Bygrave, *supra* note 277, at 571-79 (discussing the GDPRs privacy by design obligations in connection with DPIA requirements).

[281] CAL. CIV. CODE § 1798.99.31(a)(6) (West 2022); *see also* U.K. DESIGN CODE, *supra* note 1, at 57-59.

[282] *See* U.K. DESIGN CODE, *supra* note 1, at 57-59.

[283] *See id.* ("One clear example of a compelling reason is data sharing for safeguarding purposes, preventing child sexual exploitation and abuse online, or for the purposes of preventing or detecting crimes against children such as online grooming.").

[284] *See* Joseph J. Simons et al., *Competition and Consumer Protection in the 21st Century*, CTR. FOR DEMOCRACY & TECH. (Aug. 20, 2018), https://cdt.org/wp-content/uploads/2018/08/CDT-FTC-comments-5-8-20-18.pdf [https://perma.cc/AT2T-63CN] ("the FTC continues to embrace and recommend privacy by design"); FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/2DCH-GJ4R].

[285] *See* Ari Ezra Waldman, *Privacy's Law of Design*, 9 U.C. IRVINE L. REV. 1239, 1253, 1259-1285 (2019) (discussing various interpretations of privacy by design and noting that some aspects of privacy by design derive from Fair Information Practices); Ira Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1414-28 (2012) (discussing privacy by design); Waldman, *Privacy Law's False Promise*, *supra* note 265, at 794-795 (discussing privacy by design).

enforcement measures implicating this requirement can also provide guidance to companies.[286]

A privacy by design approach could be helpful in addressing some of the datafication, surveillance, and data monetization concerns discussed in Part I. Privacy by design would encourage entities to design their services with children's privacy in mind not only from the design stage, but also through the lifecycle of provided services. Thus, this approach can mitigate potential "harm upstream before it occurs, as opposed to adjusting products to reduce harm downstream after it has occurred."[287] Consideration of children's privacy at the design phase may lead companies to design services that minimize rather than enhance surveillance, thereby potentially addressing concerns associated with datafication and monetization. Privacy and security by design are critical in the IoT context and imposing such obligations on corporate actors who design and provide IoT devices, services, and software can help to minimize concerns about widespread surveillance and data collection. However, recall the California Design Act's exclusion of physical products. Privacy and security by design and default may also aid in minimizing data security risks.[288]

Like the CCPA, the U.K. Design Code and the California Design Act both incorporate data minimization principles.[289] Both

---

[286] *See* EURO. DATA PROT. BD., GUIDELINES 4/2019 ON ARTICLE 25: DATA PROTECTION BY DESIGN AND BY DEFAULT (2019), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf [https://perma.cc/F5HV-2MHT]; Avishai Ostrin, *Privacy by Design – The GDPR's Sleeping Giant*, IAPP (June 15, 2020), https://iapp.org/news/a/privacy-by-design-gdprs-sleeping-giant/ [https://perma.cc/CY9M-XXAN] (discussing the GDPR's Article 25 privacy by design obligations and European national data protection authorities' enforcement fines against corporate entities for failure to comply with the same).

[287] Camille Carlton, *Why the California Age Appropriate Design Code Is Groundbreaking*, CTR. FOR HUMANE TECH. (Sept. 29, 2022), https://www.humanetech.com/insights/why-the-california-age-appropriate-design-code-is-groundbreaking [https://perma.cc/BZ3Y-CMQ9].

[288] *See* CAVOUKIAN, *supra* note 279, at 4 (discussing the data security aspects of privacy by design).

[289] For instance, the U.K. Design Code requires companies subject to the code to "[c]ollect and retain only the minimum amount of personal data [they] need to provide the elements of [their] service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate." U.K. DESIGN CODE, *supra* note 1, at 7. It then defines "[d]ata minimization" as "collecting the minimum amount of personal data that you need to deliver an individual element of your service. It means you cannot collect more data than you need to provide the elements of a service the child actually wants to use." *Id*. at 54. Similarly, the California Design Act states companies subject to the Act should not

frameworks also specifically address problematic design features that could entice children to provide unnecessary data and authorize more uses of their personal data. The U.K. Design Code focuses on nudge techniques and restricts the use of nudge practices that "lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections."[290] Consistent with the CCPA, the California Design Act uses the term "dark patterns" and provides that companies should not use such techniques "to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections."[291]

Both the U.K. Design Code's and the California Design Act's provisions on data minimization and certain design techniques appear to align with COPPA's restriction on conditioning participation on children disclosing more data than is reasonably necessary.[292] However, the California Design Act's incorporation of several of the standards contained in the U.K. Design Code, together with the expanded age range, may allow the California Design Act to provide certain additional protections to older children in some

---

"collect . . . or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, or as described in paragraphs (1) to (4), inclusive, of subdivision (a) of Section 1798.145, unless the business can demonstrate a compelling reason that the collecting . . . or retaining of the personal information is in the best interests of children." CAL. CIV. CODE § 1798.99.31(b)(3) (West 2022). Moreover, if the "end user is a child," a company subject to the Act should not "use personal information for any reason other than a reason for which that personal information was collected, unless the business can demonstrate a compelling reason that use of the personal information is in the best interests of children." *Id.* § 1798.99.31(b)(4); *see also* Lee A. Bygrave, *supra* note 277, at 576 (noting that the GDPR's privacy by design obligations require "default application of data minimization principles, proportionality and default limits on data accessibility."); CAVOUKIAN, *supra* note 279, at 1-5 (discussing the seven foundational principles of privacy by design and noting that data minimization and privacy by default are aspects of privacy by design); Ariel Fox Johnson, *Reconciling the Age Appropriate Design Code with COPPA*, IAPP (Feb. 23, 2021), https://iapp.org/news/a/reconciling-the-age-appropriate-design-code-with-coppa/ [https://perma.cc/7YR7-Y4VR].

290 U.K. DESIGN CODE, *supra* note 1, at 8, 92 (requiring relevant companies to "not use nudge techniques to lead or encourage children to provide unnecessary personal data or turn off privacy protections" and defining those techniques as "design features which lead or encourage users to follow the designer's preferred paths in the user's decision making").

291 *Cf.* CAL. CIV. CODE § 1798.99.31(b)(7) (West 2022) *with* CAL. CODE REGS. tit. 11 § 7004(c) (defining dark pattern as a user interface that "has the effect of substantially subverting or impairing user autonomy, decision-making, or choice").

292 *See* COPPA FAQs, *supra* note 220; 16 C.F.R. 312.7.

contexts if the Act survives the current legal challenge. Additionally, while privacy by default appears to be merely a best practice under COPPA, the California Design Act is notable in that it clearly *requires* privacy by default.[293]

iv. Data Monetization Restrictions

The California Design Act and the U.K. Design Code both impose restrictions on certain types of data monetizations. The U.K. Design Code provides that children's data should not be shared without a compelling reason, but it indicates that one example "that is unlikely to amount to a compelling reason for data sharing is selling children's personal data for commercial re-use."[294] Subject to certain statutory exemptions already recognized under the CCPA, such as compliance with state and federal law, the California Design Act restricts companies from collecting, selling, retaining, and sharing personal information "that is not necessary to provide" the service that a "child is actively and knowingly engaged" with unless the firm "can demonstrate a compelling reason" that those practices are in children's best interests.[295] This restriction has the ability to

---

[293] *See* Grande, *Calif.'s Novel Privacy Moves May Dim Federal Law's* Chances, *supra* note 181 ("While COPPA focuses on obtaining parental consent and securing children's data, the design code goes well beyond the federal law to include elements such as default privacy settings"); Pixalate, *supra* note 256 ("COPPA does not specifically require privacy protective default settings for children. However, it is a best practice encouraged by the rule since operators must get verifiable parental consent before collecting personal information from children."); Avi Gesser et al., *California's Age-Appropriate Design Code Act Expands Businesses' Privacy Obligations Regarding Minors*, PROGRAM CORP. COMPLIANCE & ENF'T (Sept. 27, 2022), https://www.debevoisedatablog.com/2022/09/19/californias-age-appropriate-design-code-act-expands-privacy-obligations-for-minors/ [https://perma.cc/2D65-ZDM2] (noting that the California Design Act imposes default privacy setting obligations while COPPA does not).

[294] U.K. DESIGN CODE, *supra* note 1, at 58. The compelling reason analysis must take into account the "best interests of the child." *Id*. at 7. Notably, "[d]ata sharing usually means disclosing personal data to third parties outside your organization. It can also cover the sharing of personal data between different parts of your own organization, or other organi[z]ations within the same group or under the same parent company." *Id*. at 56.

[295] CAL. CIV. CODE § 1798.99.31(b)(3) (West 2022). However, the "obligations imposed by this title shall not restrict" the ability of a business to comply with a "court order or subpoena," among other possible exceptions. CAL. CIV. CODE § 1798.145(a)(1) (West 2022).

limit some forms of corporate data collection and data monetizations discussed in Part I of this Article.

While profiling is not banned, both frameworks provide clear restrictions on profiling by requiring companies to turn such options "off by default."[296] The California Design Act provides that covered entities should not profile children by default unless the business can show that it has adopted proper safeguards to protect children and either profiling is necessary to provide the requested services or products children are actively engaged with or the company "can demonstrate a compelling reason that profiling is in the best interests of children."[297] The U.K. Design Code contains somewhat similar provisions. To the extent that the California Design Act applies to a company's service, this restriction may limit the ease with which a company can engage in behavioral advertising using children's data, thereby potentially addressing some of the concerns discussed in Part 1. The U.K. Design Code and the California Design Act both contain somewhat similar definitions of the term profiling.[298]

---

[296] The U.K. Design Code states as follows: "Switch options which use profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing)." U.K. DESIGN CODE, *supra* note 1, at 7. However, it later notes that that this standard "does not mean that profiling is not possible or banned." *Id.* at 65. To the contrary, "[f]ollowing the safeguards and steps set out in this section, which could include effective consent, can enable profiling using children's data to take place, safely and fairly. There is no point in offering a privacy setting if the profiling is essential to the provision of the core service that the child has requested. This is because if the profiling were turned off there would be no residual service left for the child to use. This concept should be interpreted narrowly, eg that it is completely intrinsic to the service." *Id.* By comparison, the California Design Act also states that companies shall not permit profiling by default unless the "business can demonstrate it has appropriate safeguards in place to protect children" and show that "either of the following is true:" that the profiling is "necessary to provide the online service, product, or feature requested and only with respect to the aspects of the online service, product, or feature with which the child is actively and knowingly engaged" or the company "can demonstrate a compelling reason that profiling is in the best interests of children." CAL. CIV. CODE § 1798.99.31(b)(2) (West 2022).

[297] CAL. CIV. CODE § 1798.99.31(b)(2)(B)(ii) (West 2022).

[298] *Cf. id.* § 1798.99.30(b)(6) (West 2022) ("Profiling" means any form of automated processing of personal information that uses personal information to evaluate certain aspects relating to a natural person, including analyzing or predicting aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.") *with* U.K. DESIGN CODE, *supra* note 1, at 64 ("Profiling is defined in

The U.K. Design Code provides additional guidance on behavioral advertising and notes that opt-in consent is likely to be the only valid lawful basis for processing, as behavioral advertising is unlikely to qualify for a legitimate interests exception.[299] This reference to a legitimate interests exception highlights the fact that the GDPR is grounded in the notion of lawful processing.[300] This relates back to core differences between the animating documents of both legal regimes as discussed in earlier sections of this Article. It is unclear whether the term "compelling reason" in the California Design Act will be interpreted to include opt-in consent.

Similar requirements for default settings and restrictions on data collection and monetizations also apply to geolocation data and children should be notified of geolocation tracking as well as parental monitoring and tracking under both the U.K. Design Code

---

the GDPR: "any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural persons' performance at work, economic situation, health, personal preferences, interests, reliable behavior location or movements.").

[299] For instance, the U.K. Design Code instructs companies to "always provide a privacy setting for behavior[]ral advertising which is used to fund a service, but is not part of the core service that the child wishes to access." U.K. DESIGN CODE, *supra* note 1, at 65. Although behavioral advertising may be part of the core service in certain situations, such as "a voucher or 'money off' service," the U.K. Design Code nonetheless indicates these circumstances will be "exceptional." *Id*. Further, in the case of "any profiling" for "behavior[]ral advertising, which is facilitated by cookies, the comments of the EDPB guide also provide additional guidance." *Id*. at 68. To that end, the "EDPB have indicated that 'legitimate interests' is unlikely to provide a valid lawful basis for processing for this purpose which means that consent is [a firm's] only viable basis for processing. As valid consent has to be 'opt in,' allowing such profiling 'by default' is not an option." *Id*.

[300] *See* Chander et al., *supra* note 158, at 1756; GDPR art. 6(1)(a)-(f).

and the California Design Act.[301] COPPA does not appear to clearly require that companies inform minors of parental monitoring.[302]

Several provisions of the California Design Act, including monetization restrictions and those that appear to shift responsibility from parents to corporate actors and that go beyond COPPA's provisions, may raise COPPA preemption concerns for children under the age of thirteen as such provisions could be viewed as inconsistent with COPPA's framework.[303]

In *Jones v. Google LLC*, the Ninth Circuit determined that state laws that "supplement, or require the same thing, as federal law, do not stand as an obstacle to Congress' objectives, and are not 'inconsistent' . . . [and as such] COPPA's preemption clause does not bar state-law causes of action that are parallel to, or proscribe the

---

[301] For instance, it forbids companies subject to the Act from "[c]ollect[ing], sell[ing], or shar[ing] any precise geolocation information of children by default unless the collection of that precise geolocation information is strictly necessary for the business to provide the service, product, or feature requested and then only for the limited time that the collection of precise geolocation information is necessary to provide the service, product, or feature." CAL. CIV. CODE § 1798.99.31(b)(5) (West 2022). It also forbids them from collecting "any precise geolocation information of a child without providing an obvious sign to the child for the duration of that collection that precise geolocation information is being collected." *Id.* § 1798.99.31(b)(6). Moreover, if the "online service, product, or feature allows the child's parent, guardian, or any other consumer to monitor the child's online activity or track the child's location," the company must "provide an obvious signal to the child when the child is being monitored or tracked." *Id.* § 1798.99.31(a)(8). By comparison, the U.K. Design instructs companies subject to the code to "[s]witch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the bests interests of the child)." U.K. DESIGN CODE, *supra* note 1, at 7. It also requires them to "[p]rovide an obvious sign for children when location tracking is active" and "default back to off" options that make "a child's location visible to others" at the end of each session." *Id.* The U.K. Design Code defines "geolocation" as "data taken from a user's device which indicates the geographical location of that device, including GPS data or data about connection with local WIFI equipment." *Id.* at 58. By comparison, the California Design Act uses the term "precise geolocation," which the CCPA defines as "any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations." CAL. CIV. CODE § 1798.140(w) (West 2022).

[302] *See* Gesser et al., *supra* note 293.

[303] *See* 15 U.S.C. § 6502(d) (2018); Brief for Amicus Curiae Federal Trade Commission Support of Neither Party, Jones, et al., v. Google LLC, et al., No. 21-16281 (9th Cir. May 20, 2023) (discussing COPPA and preemption); Allison Grande, *COPPA Doesn't Preempt State Law*, LAW360 (May 23, 2023), https://www.law360.com/cybersecurity-privacy/articles/1680242? [https://perma.cc/M575-RBAQ] (discussing COPPA and preemption).

same conduct forbidden by, COPPA."[304] One might contend that the California Design Act simply supplements rather than contradicts COPPA's minimum requirements by imposing additional restrictions on children's personal information in a manner that permits both frameworks to seamlessly coexist. However, it is unclear whether all of the California Design Act's provisions can be viewed as supplementing or requiring "the same thing" as COPPA.

v. Detrimental Conduct Restrictions

The U.K. Design Code and the California Design Act also impose restrictions on conduct that may be harmful or detrimental to children. These restrictions appear to go beyond existing data minimization obligations and dark patterns restrictions.[305] The U.K. Design Code provides that firms should not "use children's personal data in ways that have been shown to be detrimental" to children's well-being.[306] The U.K. Design Code provides additional guidance on this standard, including recommending that companies avoid using children's data in a manner that encourages children to stay engaged, such as via the use of "personali[z]ed in-game advantages . . . in return for extended play" or suggesting that children may "lose out if they" do not continue to interact with the service.[307]

The California Design Act prohibits companies from using children's data in ways that a company "knows or has reason to know" would be materially detrimental to children's health.[308] To the extent that the California Design Act applies, this restriction has the capacity to decrease the prevalence of online services designed to encourage children to continue interacting with companies' services and products. However, the California Design Act is unlikely to apply to the physical aspects of IoT devices that may have addictive qualities for children. In addition to guidance expressly provided in the U.K. Design Code, the U.K. ICO also

---

304 Jones v. Google LLC, 56 F.4th 735, 741 (9th Cir. 2022).

305 *See* CAL. CIV. CODE §§ 1798.140, 1798.185, 1798.100(R) (West 2022).

306 U.K. DESIGN CODE, *supra* note 1, at 7 ("Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice.").

307 *Id.* at 45-47.

308 CAL. CIV. CODE § 1798.99.31(b)(1) (West 2022).

provided additional guidance with respect to detrimental data uses.[309] This guidance may be helpful in shedding light on harmful actions under the California Design Act given the reference to reliance on U.K. guidance. This may be an area in which the attorney general could, in future regulation, offer clarity on vague and undefined terms.

vi. Age Transparency Requirements

Customized-age transparency requirements are another area in which the U.K. Design Code and the California Design Act share similarities.[310] Transparency is a central tenant under the GDPR and the CCPA. Entities' privacy policies, terms and conditions and other policies and standards must be provided clearly and concisely in a manner that is suited to the ages of children who are likely to access a company's service and companies should uphold their published policies.[311] The U.K. Design Code also provides that notice should

---

309 *See* INFORMATION COMM'R'S OFF., STANDARD 5—DETRIMENTAL USE OF DATA, https://ico.org.uk/media/2620222/children-s-code-standard-5-detrimental-use-of-data.pdf [https://perma.cc/EBY5-2E3X] (last visited June 5, 2024).

310 *See* U.K. DESIGN CODE, *supra* note 1, at 37-42 ("[T]he privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child."); INFORMATION COMM'R'S OFF., DESIGNING DATA TRANSPARENCY FOR CHILDREN (2021), https://ico.org.uk/media/2620177/designing-data-transparency-for-children.pdf [https://perma.cc/JX5Q-JQRP] (providing additional guidance on the U.K. Design Code's transparency requirements); CAL. CIV. CODE § 1798.99.31(a)(7) (West 2022) ("Provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature.").

311 *Cf.* CAL. CIV. CODE § 1798.99.31(a)(7) and (9) (West 2022) *with* U.K. DESIGN CODE, *supra* note 1, at 7, 37-42 ("Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies."). The provisions of the California Design Act requiring companies to "enforce published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children" could, in theory, face First Amendment challenges akin to those faced by social media laws adopted in other states. CAL. CIV. CODE § 1798.99.31(a)(9) (West 2022); TEX. BUS. & COM. CODE § 120.052(b)(2) ("A social media platform's acceptable use policy must . . . explain the steps the social media platform will take to ensure content complies with the policy."); Netchoice v. Paxton, 49 F. 4th 439 (5th Cir. 2022); NetChoice v. AG, Fla., 34 F. 4th 1196 (11th Cir. 2022); ALTIERI & SANCHEZ, *supra* note 224 at 5 ("Florida's social media bill contains a provision that requires platforms to enforce community standards; the law is the subject of First Amendment litigation and has been appealed to the Supreme Court."). However, it is also important to note that social media laws in other states,

be provided to parents in accordance with Articles 13 and 14 of the GDPR for children younger than thirteen.[312] The obligation to enforce published policies is also arguably in keeping with another core principle of privacy by design. In addition to the other elements of privacy by design mentioned earlier, privacy by design also "seeks to assure all stakeholders that whatever the business practice or technology involved, it is, in fact, operating according to the stated promises and objectives."[313] Thus, privacy by design can be baked both into product and service development as well as corporate processes, policies, and structure with the aim of facilitating an overall privacy-centric approach.[314]

The U.K. Design Code provides additional guidance and recommendations to businesses on how to tailor their disclosures based on children's different developmental ages.[315] For example, companies could use video and audio prompts requesting that children younger than five years-old leave privacy settings as is or request help from a parent.[316] Recall that the California Design Act's preamble references similar developmental age ranges. To the extent that the California Design Act applies to a company's services, this approach to transparency has the potential to address some, but not all, concerns about the meaningfulness of consent discussed in Part I. It may increase children's understanding of companies' data practices and the possible negative implications of same as well as encourage children at a young age to understand the importance of retaining, rather than changing, privacy by default settings.

---

which require disclosure as well as explanations of editorial decisions, are quite different from the California Design Act.

312 *See* U.K. DESIGN CODE, *supra* note 1, at 40-42.

313 CAVOUKIAN, *supra* note 279, at 4.

314 *See* Ostrin, *supra* note 286 (contending that the GDPR's privacy by design obligations extend to product design as well as "organizational structure" and discussing European national data protection authorities' enforcement fines against corporate entities for failure to comply with privacy by design obligations by failing to enforce published policies).

315 *See* U.K. DESIGN CODE, *supra* note 1, at 37-42.

316 *See id*.

vii. Data Protection Impact Assessments

Unlike COPPA, both the U.K. Design Code and the California Design Act require entities to conduct DPIAs for products and services likely to be accessed by children.[317] The U.K. Design Code and the California Design Act both require that these assessments take place prior to the release of new services and products and contain guidance on the content of the DPIAs, some of which are similar.[318] For example, under both regimes, DPIAs should address, when applicable, whether the service or product may cause harm to a child by enabling exploitation or encouraging compulsive use.[319]

Notably, the U.K. Design Code indicates that it is "good practice" for companies to publish their DPIAs.[320] The California Design Act authorizes the attorney general to request access to DPIAs but provides that DPIAs are protected as confidential.[321] This authorization could be an attempt to ensure protection for companies' intellectual property rights.

The California Design Act also requires firms to review DPIAs biennially.[322] Businesses must also document any material risks caused by their data practices and establish a "timed plan to mitigate or eliminate" those risks prior to children accessing the service.[323] The U.K. Design Code also contains somewhat similar risk

---

317 *Cf.* U.K. DESIGN CODE, *supra* note 1 at 27-31 *with* CAL. CIV. CODE § 1798.99.31(A)(1)(A). *See also* Pixalate, *COPPA vs the California Age-Appropriate Design Code*, *supra* note 256 ("COPPA does not require operators to create and maintain DPIAs"); Grande, *Calif.'s Novel Privacy Moves May Dim Federal Law's Chances*, *supra* note 181 (noting that the California Design Act "goes well beyond" COPPA "to include elements such as . . . mandatory privacy assessments").

318 *Cf.* U.K. DESIGN CODE, *supra* note 1, at 29 ("You must embed a DPIA into the design of any new online service that is likely to be accessed by children. You must complete your DPIA before the service is launched, and ensure the outcomes can influence your design.") *with* CAL. CIV. CODE § 1798.99.31(a)(1)(a) (West 2022) (requiring all companies subject to the law to "complete a Data Protection Impact Assessment," prior to offering "any new online services, products, or features" to the public, for any such item "likely to be accessed by children and maintain documentation of this assessment as long as" it "is likely to be accessed by children").

319 *Cf.* CAL. CIV. CODE § 1798.99.31(a)(1)(B)(iv), (vii) (West 2022) *with* U.K. DESIGN CODE, *supra* note 1, at 30-31.

320 U.K. DESIGN CODE, *supra* note 1, at 31.

321 *See* CAL. CIV. CODE § 1798.99.31(a)(3)-(4) (West 2022).

322 *See* CAL. CIV. CODE § 1798.99.31(a)(1)(A) (West 2022).

323 CAL. CIV. CODE § 1798.99.31(a)(2) (West 2022).

mitigation provisions.[324] The California Design Act also provides that DPIAs completed for purposes of compliance with other sources of law may meet the Act's requirements. [325] This view suggests that DPIAs completed by international companies in accordance with the U.K. Design Code will likely satisfy the requirements of the California Design Act.

Arguably, DPIA obligations may raise First Amendment concerns. These requirements may amount to compelled speech because they "require[] a business to express its ideas and analysis about likely harm."[326] One response to this critique is that states can regulate economic activity and there are other sources of law that require covered entities to conduct risk analyses, document their plans and procedures, or otherwise communicate with the government regarding same.[327] Examples include legal requirements for product warnings and nutritional labels, and regulatory inspections.[328] Additionally, the statute's DPIA requirements do not appear to require companies to convey specific messages or impede any messages that a covered entity intends to send and DPIAs are confidential.[329]

III. ALTERNATIVE FEDERAL ROUTE

Recall that COPPA currently prohibits states from enacting legislation that is inconsistent with COPPA's framework. This limits states' ability to enact legislation to more adequately protect children when COPPA applies.[330] At least one state has attempted to broadly prohibit the sale of minors' personal and health information

---

[324] *See* U.K. DESIGN CODE, *supra* note 1, at 31.

[325] *See* CAL. CIV. CODE § 1798.99.31(c)(1) (West 2022).

[326] Netchoice v. Bonta, No. 22-cv-00861-BLF, 2023 LEXIS 165500, at *24 (N.D. Cal. Sept. 18, 2023); *see* Complaint for Declaratory Judgment and Injunctive Relief at 18-19, Netchoice v. Bonta, No. 22-cv-00861-BLF (N.D. Cal. Dec. 14, 2022).

[327] *See* Daniel J. Solove, *First Amendment Expansionism and California's Age-Appropriate Design Code*, TEACH PRIV. (Sept. 19, 2023), https://teachprivacy.com/first-amendment-expansionism-and-californias-age-appropriate-design-code/ [https://perma.cc/966E-XX3A].

[328] *See id.*; 26 U.S.C. §501(r)(3) (2018); Vill. of Schaumburg v. Citizens for a Better Env't, 444 U.S. 620, 637, 638 n.12 (1980); Appellant's Opening Brief at 32-26, NetChoice LLC v. Bonta, No. 23-2979 (9th Cir. Dec. 13, 2023).

[329] *See* Appellant's Opening Brief, Netchoice v. Bonta, No. 23-2969 (9th Cir. 2024) *supra* note 328, at 32-36.

[330] *See* 15 U.S.C. § 6502(d) (2018).

and prohibit the use of such data for the purpose of marketing without clear exceptions for consent.[331] The statute was ultimately repealed as portions of the law applicable to children under the age of thirteen were challenged on the grounds of COPPA preemption.[332] As discussed in Part II, some of the provisions of the California Design Act, which are applicable to children under the age of thirteen, are potentially susceptible to credible preemption challenges.[333]

In 2019, the FTC proposed revisions to the rules applicable to COPPA's framework to strengthen COPPA's protections.[334] The proposed revisions would restrict "operators' ability to send push notifications to children to prompt or encourage them to stay online longer," and impose additional limits on data retention, among other things.[335] Despite proposed changes to the COPPA rules, Congressional intervention is still needed as the FTC must work within its statutory mandate in drafting rule amendments. Congress could choose only to amend COPPA. However, recall from Part I that many of the privacy concerns that children face in the modern era stem not only from child-directed toys and devices, but also from general audience products and services. These general audience

---

331 *See* An Act to Prevent Predatory Marketing Practices Against Minors, ME. STAT. tit. 10, § 9551 et seq. (repealed 2009); 3 JAMES ASTRACHAN ET AL., THE LAW OF ADVERTISING § 56.05[3] (LexisNexis 2022) (noting that the Maine statute did "not provide for any exceptions to its prohibition of collection and/or use of a minor's health-related or personal information for marketing purposes without verifiable parental consent, as provided under COPPA").

332 *See* Ian Ballon, *Maine's [Now Repealed] Predatory Marketing Practices Against Minors Act*, in 3 IAN BALLON, E-COMM. & INTERNET L. (2020); *Marketing to Minors in Maine*, PROMOLAW, https://www.promolaw.com/news-resources/2017/11/27/marketing-to-minors-in-maine [https://perma.cc/P7XV-JPSK] (last visited July 16, 2021).

333 *See, e.g.*, Complaint for Declaratory Judgment and Injunctive Relief at 25-26, Netchoice v Bonta, No. 22-cv-00861-BLF (N.D. Cal. Dec. 14, 2022).

334 *See* Allison Grande, *FTC Targets Data Profits With Kids' Privacy Rule Changes*, LAW360 (Dec. 20, 2023), https://www.law360.com/technology/articles/1779564? [https://perma.cc/F6MR-N6W7].

335 *See id.*; Press Release, Alvaro M. Bedoya, Comm'r, Fed. Trade Comm'n, Statement on the Issuance of the Notice of Proposed Rulemaking to Update the Children's Online Privacy Protection Rule (COPPA Rule) (Dec. 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/BedoyaStatementonCOPPARuleNPRMFINAL12.20.23.pdf [https://perma.cc/HX3R-TL3Q]; Lesley Fair, *FTC Proposes Enhanced Protections for Kids Online. Where Do You Stand?*, FED. TRADE COMM'N (Dec. 20, 2023), https://www.ftc.gov/business-guidance/blog/2023/12/ftc-proposes-enhanced-protections-kids-online-where-do-you-stand [https://perma.cc/4CQ8-KNVH].

devices may not always be subject to COPPA's framework absent satisfaction of COPPA's actual knowledge requirements.[336]

Additionally, various technological developments, including the IoT, advanced machine-learning algorithms and companies' unprecedented rate of data collection and disclosures, highlight the pressing need for privacy legislation at the federal level to protect both minors and adults. In 2022, there was some progress towards the adoption of a comprehensive data privacy statute—the American Data Privacy and Protection Act.[337] In 2024, the "heads of the U.S. Senate and House commerce committees" reached an agreement on a bipartisan draft of the proposed American Privacy Rights Act.[338] It is too early to tell whether the 2024 bill will succeed in contrast to the 2022 bill.

If Congress elects to seriously consider adopting federal baseline privacy legislation, it could address the special needs of children in the connected age in such a statute and consider the ways in which existing protections under COPPA's framework can be enhanced, incorporated or replaced. As former acting chair of the FTC Maureen K. Ohlhausen has observed, "sensitive personal information, such as health and financial information, real-time precise geo-location information, social security numbers, and children's information, poses the highest risk of consumer harm and should be subject to the highest protections."[339] If Congress intends to adopt a comprehensive privacy statute, the resulting legislation should address privacy and security concerns in the IoT and non-IoT context. Adoption of a comprehensive statute has the added benefit of correcting the U.S. sectoral approach to privacy, while also

---

[336] *See* COPPA FAQS, *supra* note 220 ("[T]he [COPPA] Rule also applies to operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under [thirteen], and to websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children.") (alteration in original).

[337] *See* American Data Privacy and Protection Act, H.R. Res. 8152, 117th Cong. (2022).

[338] Grande, *Key Congressional Leaders Float Sweeping Data Privacy Bill*, *supra* note 26; *see* APRA, *supra* note 26. This bill, if enacted, will expand on the American Data Privacy and Protection Act. *Data Privacy Strikes Back: American Privacy Rights Act*, BROWNSTEIN (Apr. 11, 2024), https://www.bhfs.com/insights/alerts-articles/2024/data-privacy-strikes-back-american-privacy-rights-act [https://perma.cc/E89S-JWP9].

[339] Congress Should Enact a National, Comprehensive Consumer Privacy Framework: Hearing Before the S. Comm. on Com., Sci., and Transp., 116th Cong. 6 (2019) (statement of Maureen K. Ohlhausen, Former Acting Chair of FTC).

having the capacity to address privacy issues that impact both children and adults.

Admittedly, there are several obstacles to the adoption of baseline federal privacy legislation, including disputes about whether any such statute (i) should preempt more protective state laws,[340] (ii) will provide adequate protections for personal data considering companies' strong lobbying efforts, (iii) should include a private right of action and (iv) will effectively deal with existing federal sectoral legislation. The GDPR and some aspects of the CCPA and the California Design Act could be useful sources for drafting federal baseline legislation. To the extent that the GDPR's provisions are considered for incorporation into a federal statute they will need to be adjusted to accommodate the U.S. legal landscape.[341]

---

[340] On the issue of preemption, its federal baseline privacy legislation could adopt the approach taken in the Clean Air Act and amendments which permitted California to adopt more stringent standards and allowed the state "to use its developing expertise in vehicle pollution to develop innovative regulatory programs." 42 U.S.C.A. §7543(b)(1) (West 2022); Rachel L. Chanin, *California's Authority To Regulate Mobile Source Greenhouse Gas Emissions,* 58 N.Y.U. ANN. SURV. AM. L. 699 (2003) ("[T]he Clean Air Act permits states to opt into California's more stringent emissions regulation program."); Matthew Visick, *If Not Now, When? The California Global Warming Solutions Act of 2006: California's Final Steps Toward Comprehensive Mandatory Greenhouse Gas Regulation*, 13 HASTINGS W.-N.W. J. ENV. L. & POL'Y 249 (2007) ("Clean Air Act regulates air pollutants from vehicular sources uniformly . . . . Section 209(a) of the Clean Air Act expressly preempts state regulation of vehicular sources. An exception to section 209(a) is made in section 209(b) for California, which may adopt its own air pollution standards after applying for and obtaining an EPA waiver. For California to be eligible for a waiver, it must first determine that its standards 'will be, in the aggregate, at least as protective of public health and welfare as applicable Federal standards.'"); *see* Danielle Keats Citron & Alison Gocke, *Nancy Pelosi Is Blocking Landmark Data Privacy Legislation – for a Good Reason*, SLATE (Sept. 9, 2022), https://slate.com/technology/2022/09/nancy-pelosi-data-priavcy-law-adppa.html [https://perma.cc/6SK9-PZ4K].

[341] *See* ELVY, A COMMERCIAL LAW OF PRIVACY, *supra* note 55, at 279-91, 312 ("If GDPR-like principles are imported, the [United States] can learn from the GDPR's deficiencies and adapt federal legislation and regulation."). For instance, a GDPR-like right to delete in the United States can be inspired by the EU's right to be forgotten, but given First Amendment concerns, such a right may need to be narrowly tailored.

a. Minimizing Data Acquisition and Surveillance

Given concerns related to notice and choice and privacy-self management discussed earlier, federal legislation should not rely solely on granting individuals data rights, such as the right to access or delete data. Congress could require rather than merely recommend that companies adopt data minimization principles and privacy and security by default and design when creating online products and services.[342] Data retention limitations could also be imposed. Data minimization and retention limits may aid in addressing some civil liberties concerns by decreasing data collection, surveillance and opportunities for subsequent uses and disclosures. The American Law Institute's Principles of Law, Data Privacy ("ALI Data Privacy Principles") also contain privacy and security by design and default principles.[343]

Other provisions of the California Design Act may also be useful in drafting a federal privacy statute. For instance, like the California Design Act, restrictions can also be imposed on design techniques that encourage children to continue to interact with websites and products. Federal privacy legislation could also combine baseline data rights, data minimization and privacy and security by design and default obligations with a duty of loyalty that requires companies to act in the best interest of data subjects.[344] Various scholars have advocated for such a duty. Neil Richards and Woodrow Hartzog, for instance, have described in detail what such a duty would require and how to implement the same.[345] Such a

---

[342] *See* Neha Mishra, *Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?*, 19 WORLD TRADE REV. 341, 358 (2020) ("The EU has included a mandatory privacy requirement and security by design in the GDPR.").

[343] *See* PRINCIPLES OF THE LAW—DATA PRIVACY § 13(d)-(e) (AM. L. INST. 2020).

[344] *See* Richards & Hartzog, *supra* note 263, at 1017 ("We are not advocating for a duty of loyalty in privacy law *in place* of a robust data protection regime. We are arguing for a duty of loyalty *in addition* to it. One of the hallmarks of the GDPR is that the obligations regarding collection and processing follow the data downstream. While loyalty might only apply within the confines of a relationship, data protection rules apply to everyone that touches the data. In this way, the powerful but incomplete protections of both a data protection and a data loyalty approach can complement each other nicely.").

[345] *See* Richards & Hartzog, *supra* note 263; *see also* SOLOVE, *supra* note 274, at 102-04; ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 8 (Cambridge Univ. Press 2018); Balkin & Zittrain, *supra* note 274. Professors Richards and Hartzog note that a "breach of a duty of loyalty would be a per se legal injury that could solve the standing problem that has plagued privacy

duty could aid in correcting the overreliance on notice and choice and foster the development and design of products that are more privacy-protective. Imposing such a duty regardless of the data subjects' age could avoid age assurance concerns that might arise when similar duties are made applicable only to children. Adopting legislation that provides baseline privacy rights in combination with privacy and security by default obligations as well as a duty of loyalty could also protect data submitted by parents about children. Recall that COPPA generally does not extend its protections to such data. Admittedly, a proposal for a duty of loyalty in the privacy context has received its fair share of criticism, including that such a duty may raise First Amendment concerns.[346] Despite the potential

---

litigation," particularly since "*Spokeo* and *Ramirez* require a concrete legal injury." Richards & Hartzog, *supra* note 263, at 1012. Further, since "English and American courts have recognized" such breaches "in the fiduciary context for hundreds of years, an alleged breach of a duty of loyalty would satisfy the Spokeo/Ramirez test under its express terms." *Id*. It is possible that imposition of an obligation to act in the best interest of the child could pose less significant standing and First Amendment concerns when compared to the data trade restrictions discussed in earlier sections of this article. For instance, Professor Balkin discusses a proposed duty of loyalty for information fiduciaries and contends that "the First Amendment does not prevent the state from regulating how professionals interact with their clients and how they use their clients' information" since "professionals have a fiduciary relationship with their clients." Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1161 (2018). He further contends that courts "are more likely to treat restrictions on collection or use as not raising First Amendment questions at all, because they aim at conduct. In the alternative, courts may treat them as content neutral time, place, and manner regulations. The most serious First Amendment problems usually arise on the back end when governments try to regulate disclosure, distribution, and sale of information." Balkin, *The Fiduciary Model of Privacy*, *supra* note 275, at 30. Professor Balkin has discussed this same issue elsewhere. *See, e.g.*, Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 274, at 1186; Jack Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014), https://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [https://perma.cc/95MF-9HYH] (discussing the information fiduciary framework and duty of loyalty). Professor Richards similarly observes that rules "placing nondisclosure obligations on data processors will rarely place burdens on First Amendment values, especially if they are couched as confidentiality rules." Neil Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1512 (2015).

346 For instance, in response to Jack Balkin's information fiduciary framework, Professor Bhagwat contends that the framework has "a serious constitutional problem, rooted in the First Amendment. The problem, in short, is that the current Supreme Court has strongly suggested that it considers the transfer and sale of data to be speech. As such, restrictions on the sale of data (especially if anonymized, as in effect it is when social media firms sell advertising)." Bhagwat, *supra* note 117, at 2384-85. Others have made similar criticisms. *See, e.g.*, Harold Feld, *Privacy Legislation, Not Common Law Duties*, L. & POL. ECON. PROJECT (July 4, 2019),

benefits of imposing such a duty regardless of age, courts may be more willing to uphold such a duty if it is limited to children given the strong and compelling legislative interest in protecting children.

b. Market Deterrent Restrictions and Consent Timing

Congress could also consider additional restrictions on data monetizations and limit the role of consent. To better deal with rampant corporate data monetization, the failings of the notice and choice model and opt-out mechanisms, power imbalances and information asymmetry in the digital era, several scholars have proposed limits on alienability or limitations on the effectiveness of consent. Although consumers cannot be said to have a traditional "property interest" in their data, Walter Miller, Jr. and Maureen A. O'Rourke have contended that:

> [T]here may be some information that should be inalienable because of its highly personal nature . . . and [a] legal rule of inalienability may be appropriate for some types of highly personal information, not only when the data collector has promised not to disclose such data, but also even if the customer is willing to permit its transfer.[347]

---

https://lpeproject.org/blog/privacy-legislation-not-common-law-duties/ [https://perma.cc/89QJ-WQYJ].

347 Walter W. Miller, Jr. & Maureen A. O'Rourke, *Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card?*, 38 HOUS. L. REV. 777, 847 (2001); *see also* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1132 (2000) ("[H]owever intuitively powerful the notion of property rights in one's data may be, it is clear that in the [United States] the existence of some legally protectable interests in personal data in certain circumstances is not equivalent to a legal rule that a person has a property interest in one's personal data."). Case law has also made this clear. *See, e.g.*, In re Facebook Privacy Litig., 791 F. Supp. 2d 705, 714 (N.D. Cal. May 12, 2011), *aff'd in part*, Facebook Privacy Litig. v. Facebook, Inc., 572 F. App'x 494 (9th Cir. 2014) (holding that "personal information does not constitute property for purposes of" a claim under California's Unfair Competition Law); Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1126–27 (N.D. Cal. 2008), *aff'd*, 380 Fed. Appx. 689 (9th Cir. 2010) (finding that plaintiff did not present "any authority to support the contention that unauthorized release of personal information constitutes a loss of property"); *see also* John M. Newman, *Anti-Trust in Zero-Price Markets: Applications*, 94 WASH. U. L. REV. 49, 55 (2016) ("[C]ourts have been uniformly reluctant to treat personal information as property for general legal purposes."). Anita Allen has also argued that, "in an egalitarian liberal democracy, particularly if justified on broadly dignitarian grounds, legal policy makers . . . must be open, in principle, to coercive privacy mandates that impose unpopular privacies on intended targets and beneficiaries." ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? xii

Paul Schwartz has proposed a "hybrid inalienability [model] consisting of a use-transfer restriction."[348] Somewhat similarly and more broadly, Nancy Kim's consentability framework evaluates in part under what circumstances "the state should exercise its power to prevent an individual from consenting."[349]

Following the above points and considering the vulnerable nature of children and the unprecedented speed at which companies can monetize children's data, Congress could attempt to restrict the market for certain types of data it deems as needing heightened protections. Such an approach may be preferable considering the noted ineffectiveness of the notice and consent model. Also, consider that a 2021 report on child data privacy found that "[s]elling data, often considered one of the worst practices, has increased over the past four years," which increases the privacy risks children and their families face.[350] To be clear, this Article does not contend that there is absolutely no value in providing notice and offering parents and children a choice. Rather, it highlights the limits of depending excessively on the notice and choice model to adequately protect children's interests. While some aspects of the notice and choice model can be retained in federal privacy legislation, Congress, in some instances, could move beyond notice and choice by, for instance, imposing market deterrent restrictions on certain types of data regardless of consent. Given First Amendment concerns and the potential compelling government interest in protecting children's privacy, Congress could decide to impose such restrictions on certain types of child data. Congress may also need to consider whether any such restrictions should apply to anonymized and aggregated data. Recall the potential weaknesses of anonymization discussed in Part I. However, restrictions on anonymized data may pose even greater First Amendment concerns.

(Oxford Univ. Press 2011); *see also* Richards & Hartzog, *supra* note 263, at 998 ("[D]uties of loyalty would align with Anita Allen's proposal for coercive privacy mandates that prohibit waiver.").

348 Paul M. Schwartz, *Property, Privacy, And Personal Data,* 117 HARV. L. REV. 2055, 2060 (2004).

349 NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS 53 (Cambridge Univ. Press 2020).

350 Press Release, Common Sense Media, New Report from Common Sense Media Assesses Privacy Policies of Hundreds of Education and Consumer Tech Apps and Services (Nov. 17, 2021), https://www.commonsensemedia.org/press-releases/new-report-from-common-sense-media-assesses-privacy-policies-of-hundreds-of-education-and-consumer-tech [https://perma.cc/NQ8Z-KGZC].

Market deterrent restrictions are not new to American privacy law. BIPA relies in part on notice-and-consent mechanisms for the collection of biometric identifiers. However, BIPA also prohibits companies from selling, trading or profiting from biometric identifiers without providing an express exception for consent to such activities, even though the statute allows a company to collect such data if it first "receives a written release executed by" the consumer, among other things.[351] Thus, under BIPA it appears that, although a company may collect biometric identifiers directly from an individual with consent, a company may not subsequently "sell, lease, trade or otherwise profit from" those data.[352] This prohibition appears to serve as a secondary data trade or market deterrent restriction. Additionally, BIPA's private right of action gives teeth to the statute's notice and consent requirements. To this end, the Seventh Circuit pointed out that BIPA has a "prohibition against for profit transactions" that involve biometric identifiers,[353] while several legal practitioners and commentators in this area have further noted that, under BIPA, companies may not sell, lease or profit from biometric identifiers "regardless of any disclosure or consent."[354] Similarly, in 2021 a district court evaluating BIPA's

---

351 *See* 740 ILL. COMP. STAT. ANN. 14/15 (2022).

352 *Id.*

353 *See, e.g.*, Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1247 (7th Cir. 2021).

354 P. Russell Perdew, *Biometric Information Privacy Act (BIPA): A Checklist for Defendants*, LOCKE LORD (Nov. 9, 2017), https://www.lockelord.com/newsandevents/publications/2017/11/biometric-information-privacy-act [https://perma.cc/6LV6-B423]. One firm advises companies "collecting biometrics as defined by BIPA" to "evaluate [the] practices for compliance," specifically instructing firms to "stop immediately" if they "sell, lease, trade, or otherwise profit from a person's biometrics." *Id.*; *see also* Joshua Valentino, *Setting the Framework for Biometric Privacy Legislation After the "Big Bang" of Biometrics in the Workplace*, 38 HOFSTRA LAB. & EMP. L.J. 167, 178 (2020) ("[O]nly BIPA prohibits the sale of biometric information without exception."); Anjelica Cappellino, *The Illinois Biometric Information Privacy Act: What Makes a Winning Case?*, EXPERT INST. (May 27, 2021), https://www.expertinstitute.com/resources/insights/the-illinois-biometric-information-privacy-act-what-makes-a-winning-case/ [https://perma.cc/PES2-9G5Z] ("The BIPA prohibits any private entity from selling the data, even with consent."); Theodore F. Claypoole & Cameron S. Stoll, *State Forays into the Regulation of Biometric Data*, LAW360 (Nov. 10, 2015), https://www.law360.com/articles/724349/state-forays-into-the-regulation-of-biometric-data [https://perma.cc/YQS2-U3GM] ("Whereas BIPA prohibits an entity from profiting from biometric data it collects, the Texas law allows a party to sell, lease or disclose biometric identifiers under a narrow set of circumstances."). *But see* Vigil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499 n.9 (S.D.N.Y. 2017) ("In relation to the other terms in Section 15(c)—'selling' 'leasing,' and 'trading'—'otherwise profiting' is a catchall for prohibiting commercially

secondary data trade restrictions noted that "unlike the collection, possession or dissemination of biometric data, no private entity may [sell, lease or trade or] otherwise profit from biometric data [under BIPA] even if they inform and obtain permission from the subject."[355]

Despite the merits of the above-referenced proposal, as I have noted elsewhere, the First Amendment may pose a significant obstacle to the adoption of trade, marketing, or use restrictions in the consumer data context.[356] In *Sorrell v. IMS Health Inc.*, the Supreme Court held that a Vermont statute that restricted certain entities' ability to sell or use anonymized "prescriber-identifying information" for "marketing or promoting a prescription drug" without prescriber consent "impose[d] content- and speaker-based burdens on protected expression [and was] subject to heightened judicial scrutiny."[357] Scholars disagree on the implications of the *Sorrell* decision.

Some scholars have suggested that the opinion means that "the transfer and sale of data" is protected speech under the First Amendment.[358] Other scholars contend that the Supreme Court

---

transferring biometric information and biometric identifiers in a manner not contemplated by the original biometric-facilitated transaction, without consent from the individual pursuant to Section 15(d).").

355 Vance v. Amazon.com Inc., 534 F. Supp. 3d 1314 (W.D. Wash. 2021) (discussing BIPA's prohibitions on the sale of biometric data). *Cf.* 740 ILCS 14/15(d) (allowing dissemination of biometric data with consent from subject) *with* 740 ILCS 14/15(c) (containing no exceptions).

356 *See* ELVY, A COMMERCIAL LAW OF PRIVACY, *supra* note 55, at 293-94; Elvy, *Commodifying Consumer Data*, *supra* note 28, at 396. Another potential critique of such proposals is that they may interfere with parents' ability to consent on behalf of and resolve issues for their children. The Supreme Court's holding in *Troxel v. Granville* seemingly recognizes such a right. *See Troxel v. Granville*, 530 U.S. 57, 65 (2000) ("[T]he interest of parents in the care, custody, and control of their children – is perhaps the oldest of the fundamental liberty interests recognized by this Court. More than 75 years ago, . . . we held that the 'liberty' protected by the Due Process Clause includes the right of parents to establish a home and bring up children [and we] confirmed that there is a constitutional dimension to the right of parents to direct the upbringing of their children.") (alteration in original). One response to this critique is that parents' rights in this area is not entirely absolute and my proposal is, to some extent, in keeping with this approach. Additionally, minors have their own constitutional rights in some areas. *See, e.g.*, Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 603 (1969).

357 Sorrell v. IMS Health Inc., 564 U.S. 552, 552-59 (2011).

358 Bhagwat, *supra* note 117, at 2384-85 ("[R]estrictions on the sale of data (especially if anonymized, as in effect it is when social media firms sell advertising) poses serious First Amendment challenges."); *see also* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 71 (2014) (contending that part of the Sorrell "opinion suggested that the restriction on transfers of data between willing givers and

"stopped short of [the] sweeping conclusion" that database sales are speech.[359] Neil Richards contends that "Sorrell discriminated against particular kinds of protected speech (in-person advertising), and particular kinds of protected speakers (advertisers but not their opponents) . . . [and] the real problem with the Vermont law at issue was that it didn't regulate enough."[360] Along those lines, Jack Balkin posits that after *Sorrell* First Amendment concerns may occur when the legislative branch focuses privacy laws only at certain classes of companies.[361] The *Sorrell* Court also did not adequately consider the potential risk of de-anonymization.[362]

Given the varying interpretations of the *Sorrell* opinion, it does not appear with absolute certainty that well-drafted secondary trade restrictions enacted as part of a comprehensive and "coherent policy" on "generally applicable" consumer data protection will run afoul of the First Amendment.[363] Arguably BIPA is one such

---

receivers was automatically a restriction of speech"); Ashutosh Bhagwat, *Sorrell v. IMS Health: Details, Detailing, and the Death of Privacy*, 36 VT. L. REV. 855, 856 (2012) (suggesting that "hints" left by the Sorrell court may negatively impact the validity of rules aimed at protecting privacy); Alexander Tsesis, *Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure*, 90 U. COLO. L. REV. 593, 617 (2019) ("[T]he commercial reselling of supposedly anonymized data that was the subject of litigation in Sorrell v. IMS [was] struck down on First Amendment grounds a statute that had prohibited data mining in pharmaceutical prescription files.").

359 Richards, *supra* note 345, at 1506, 1521-24 (2015) ("Before Sorrell, there was a settled understanding that general commercial regulation of the huge data trade was not censorship. On the contrary, it was seen as part of the ordinary business of commercial regulation that fills thousands of pages of the U.S. Code and the Code of Federal Regulations. Nothing in the Sorrell opinion should lead policymakers to conclude that this settled understanding has changed.").

360 *Id.*

361 *See* Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 274, at 1186.

362 *See* Tsesis, *supra* note 357, at 617 (discussing Sorrell and noting that "the majority did not take into account that even the sale of anonymized personal information is not safe from resale to third-party vendors who can then deanonymize"). *But see* Jane Yakowitz & Daniel Barth-Jones, *The Illusory Privacy Problem in Sorrell v. IMS Health* (Tech. Pol'y Inst., 2011), https://techpolicyinstitute.org/wp-content/uploads/2011/05/the-illusory-privacy-problem-i-2007545.pdf [https://perma.cc/PR7K-C6GJ] (minimizing the risk of de-anonymization).

363 NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 13, 23 (Oxford Univ. Press 2016) ("[C]onfidentiality rules that regulate the obligations of parties to a relationship rather than whether a fact can be published by anyone pose even fewer First Amendment problems . . . [and] restrictions on the sale of targeted marketing lists under the Fair Credit Reporting Act have survived First Amendment attack, with the Supreme Court declining to get involved.").

example. Thus, it is possible that legislators may have room to adopt such restrictions until such time as the Supreme Court clearly indicates otherwise. At least one court has found that BIPA's provisions do not violate the First Amendment using intermediate scrutiny.[364]

In *Thornley v. Clearview AI, Inc*., the Seventh Circuit dismissed the case for lack of standing, but suggested that BIPA's sale restrictions were similar to other trade or market-deterrent based restrictions that the Supreme Court previously upheld.[365] The court observed that regulations under the Migratory Bird Treaty Act[366] and the Eagle Protection Act[367] authorize "the possession or transportation of certain migratory birds, and their parts, nests, or

---

364 *See* ACLU v. Clearview AI, Inc., No. 20 CH 4353, *2021 Ill. Cir. LEXIS 292* at *20, *25 (*Ill. Cir.* Ct. Aug. 27, *2021*) (because "BIPA's speaker-based exemptions do not appear to favor any particular viewpoint. As BIPA's restrictions are content neutral, the Court finds that intermediate scrutiny is the proper standard" and, moreover, that "BIPA's restrictions on Clearview's First Amendment freedoms are no greater than what's essential to further Illinois' interest in protecting its citizens' privacy and security."). The court there distinguished *Sorrell* by reasoning that, unlike BIPA, "speaker-based distinctions should lead to strict scrutiny only if those exemptions are hiding content- or viewpoint-based preferences. In *Sorrell*, the court found that a speaker-based distinction (regulating who could and who could not talk about certain drugs) reflected a viewpoint-based distinction in favor of speech promoting generic drugs. In summarizing its holding, the court focused on the effect of the law on suppressing certain ideas" *Id*. at *20. In the subsequent class action, the court again applied intermediate scrutiny, reasoning that "Clearview's process in creating its database involves both speech and nonspeech elements. When these 'elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms.'" In re Clearview AI, Inc., Consumer Priv. Litig., 585 F. Supp. 3d 1111, 1120 (N.D. Ill. 2022) (citing U.S. v. O'Brien, 391 U.S. 367, 376 (1968)). Applying this standard, the court found that it passed the third prong of O'Brien that requires "a governmental interest" that "is unrelated to the suppression of free expression" because "BIPA, including its exceptions, does not restrict a particular viewpoint nor target public discussion of an entire topic." *Id*. at 1121. Pasquale suggests that, assuming firms' data practices even deserve free expression protections, restrictions on them "may be subject to only intermediate scrutiny," the level of scrutiny he views as appropriate in light of the "privacy and security concerns raised by mass data collection, analysis, and use." Frank Pasquale, Licensure as Data Governance, KNIGHT FIRST AMEND. INST. (Sept. 28, 2021), https://knightcolumbia.org/content/licensure-as-data-governance [https://perma.cc/E7N2-5WCZ]; *see also* Ben Kochman, *Clearview Can't Use 1st Amendment to Beat Ill. Privacy Suit*, LAW360 (Aug. 27, 2021 9:28 PM), https://www.law360.com/articles/1417184 [https://perma.cc/K8E6-9AR9] (discussing the procedural posture of the Clearview case).

365 *See Thornley*, 984 F.3d at 1241, 1242, 1247.

366 *See* 16 U.S.C. § 703 (2018).

367 *See id*. § 668 (2018).

eggs, but they state that these items 'may not be imported, exported, purchased, sold, bartered, or offered for purchase, sale, trade, or barter.'"[368] The Seventh Circuit reasoned that the Supreme Court interpreted these provisions "as a regulatory prohibition against commerce in the covered birds and bird parts, and it upheld the [associated] regulations."[369] However, while the sale of bird parts may be viewed as conduct, data could arguably constitute speech. In *Sorrell*, the state argued that restrictions on the sale and transfer of prescriber identifying information were conduct as opposed to speech.[370] Similarly, the lower court in *Sorrell* "characterized prescriber-identifying information as a mere 'commodity' with no greater entitlement to First Amendment protection than 'beef jerky.'"[371] In response to this argument, the Supreme Court noted in *Sorrell* that "the creation and dissemination of information are speech within the meaning of the First Amendment."[372]

Despite the potential concerns with the bird analogy mentioned earlier, the Seventh Circuit's opinion in *Thornley* also reveals another important benefit of market restrictions. Such restrictions may also indirectly help in addressing concerns about surveillance and data collection. In evaluating BIPA's market-based restrictions, the Seventh Circuit reasoned that if "it is not profitable to collect or hold [biometric] data [due to sale restrictions], one can assume that the incentive to collect it or hold it will be significantly reduced."[373]

Rather than imposing data trade restrictions, Congress could consider attempting to specifically regulate the timing of consent and require separate consents for certain types of data monetization's with the hope that such restrictions may increase

---

[368] *Thornley*, 984 F.3d at 1247 (citing Andrus v. Allard, 444 U.S. 51, 54 (1979)). In *Allard*, the Court held that "the prohibition against the sale" of "pre-existing avian artifacts" did not constitute a "taking" of the artifact owners' property in violation of the Fifth Amendment because, although the regulations "prevent[ed] the most profitable use" of their property, that fact "is not dispositive," particularly since they "retain[ed] the rights to possess and transport their property, and to donate or devise it." *Allard*, 444 U.S. at 66-68.

[369] *Thornley*, 984 F.3d at 1247. The Seventh Circuit also noted that the parties did not contend that BIPA violated "the Takings Clause, substantive due process, or a federal statute." *Id.* As a result, the court did not express an opinion on these issues. *See id.* Perhaps this statement suggests that BIPA's sale prohibitions as well as the secondary trade restrictions discussed earlier may be vulnerable to other constitutional and federal statutory challenges.

[370] *Sorrell*, 564 U.S. at 558.

[371] *Id.*

[372] *Id.* at 559.

[373] *Thornley*, 984 F.3d at 1247.

parents' and children's understanding of companies' data practices and address concerns with the existing notice and choice model. Stated differently, a parent might consent to the collection of their child's data by an initial data collector, but the initial data collector could be prohibited from subsequently selling the data to third parties if consent to the subsequent transaction is not obtained at the time of or closer in time to the subsequent sale to a third party. Additionally, Congress could require separate consents for behavioral advertising and build on existing provisions in COPPA by imposing limits on the ability of entities to condition access to their products on the disclosure of data to unrelated entities.[374]

The ALI Data Privacy Principles appear to adopt a somewhat similar approach to consent timing with respect to certain data activities. The principles note that, in some cases, heightened notice is recommended[375] and such notice should "be made more prominently than ordinary notice and closer in time to the particular data activity."[376] Other sources of law also have restrictions on the timing of consent. For instance, Article 9 of the UCC provides that a debtor may consent to "waive the right to notification of disposition of collateral . . . only by an agreement to that effect entered into and authenticated after default."[377]

---

[374] *See, e.g.*, Press Release, FED. TRADE COMM'N, FTC Proposes Strengthening Children's Privacy Rule to Further Limit Companies' Ability to Monetize Children's Data (Dec. 20, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens [https://perma.cc/KRQ4-QV8T].

[375] *See* PRINCIPLES OF THE LAW—DATA PRIVACY, *supra* note 343, § 4(e)(1).

[376] *Id.* § 4(e)(6); *see also id.* § 5 (discussing heightened consent requirements). Professor Solove discusses the trigger that these "Principles" provide for "heightened notice. Daniel J. Solove, *ALI Data Privacy: Overview and Black Letter Text*, 68 UCLA L. REV. 1252, 1271 (2022). In particular, he notes that heightened notices apply to "any data activity that is significantly unexpected or that poses a significant risk of causing material harm to data subjects." *Id.* (citing PRINCIPLES OF THE LAW—DATA PRIVACY, *supra* note 343, § 4(e)(1)). In such cases, Professor Solove argues, "[h]eightened notice should be more conspicuous, such as a 'pop up' that appears at the moment a data activity is about to occur." *Id.*

[377] U.C.C. § 9-624 (AM. L. INST. & UNIF. L. COMM'N 2023); *see also* LINDA RUSCH & STEPHEN SEPINUCK, PROBLEMS AND MATERIALS ON SECURED TRANSACTIONS (Thomson West 2010) ("No obligor, primary or secondary, may waive the rights listed in § 9-602 prior to default."); JAMES J. WHITE & ROBERT S. SUMMERS, UNIFORM COMMERCIAL CODE 1326 (6th ed. 2010) ("Section 9–602 contains a list of sections that "give rights to a debtor . . . and impose duties on a secured party." To the extent of those rights and duties, the debtor may not waive or vary those sections."); Wayne R. Barnes, *Confidentiality Clauses in Settlement Agreements After the Consumer Review Fairness Act*, 50 FLA. ST. U. L. REV. 469, 506 (2023) ("Article 9 allows for some agreements (*e.g.*, settlement agreements) to waive the right of redemption, so long

One possible critique of consent timing restrictions is that companies could simultaneously obtain consent to data collection and data sales at the same time if the corporate data trade occurs immediately at the time of the initial data collection, which would render the timing restriction less meaningful. This critique perhaps lends support for broader secondary trade restrictions that do not depend on the timing of consent. Secondary trade restrictions are also, to some extent, in keeping with recommendations by other scholars in support of limiting data collection.[378] Additionally, as Ari Ezra Waldman observes, to effectuate true change in the privacy law field that more adequately tackles corporate influence and power, "privacy law should also start becoming more comfortable with two words that are gaining increasing prominence among scholars and advocates: 'ban it.'"[379] Other scholars have also urged Congress to adopt "outright prohibitions" on the sale of certain types of data.[380]

Historically, when faced with major societal changes our legal system responded, in some cases, with express restrictions on trade, with the seeming understanding that adequate protection of individuals is likely to be best achieved through the adoption of such restrictions. For instance, the law restricts the sale and purchase of human organs for "valuable consideration," even if consent is received.[381] While the civil and criminal contexts are different, there has been at least one proposal at the state level to criminalize (as a misdemeanor) the collection of certain types of consumer data

---

as they are far *subsequent* to the initial contract (in Article 9's case, not until after default on the secured obligation/loan"). *Cf.* U.C.C. § 9-603 (AM. L. INST. & UNIF. L. COMMN.) (allowing agreements to set the standards by which some of the secured party's duties and the parties rights will be measured) *with id.* § 9-624 (allowing certain rights to be waived after default).

[378] *See* Hartzog & Richards, *supra* note 167, at 1753 (contending that lawmakers "can get serious about limiting collection in the first place. Some scholars have argued that since the internet's creation, the restrictions on data collection are equally (and sometimes more) important than rules surrounding data use").

[379] ARI EZRA WALDMAN, INDUSTRY UNBOUND 239 (Cambridge Univ. Press 2021).

[380] Statement of Justin Sherman, *supra* note 119, at 6 ("Congress should develop a set of strict controls on data brokers' sales of data to foreign companies, citizens, and governments—weighing outright prohibitions in some cases (*e.g.*, on selling data on government employees and military personnel).").

[381] *Cf. with* National Organ Transplant Act, 42 U.S.C. § 274e(a) (2018) ("It shall be unlawful for any person to knowingly acquire, receive, or otherwise transfer any human organ for valuable consideration for use in human transplantation if the transfer affects interstate commerce.").

without consent.[382] We have reached an inflection point with children's data as companies amass even more data about children from a young age than ever before. This significant societal and technological shift necessitates bold responses by legislators.

c. IoT Specific Obligations

With respect to IoT toys and other devices, in contrast to the approach taken in the California Design Act, federal privacy legislation should clearly bring IoT devices within its scope. As part of their privacy and security by design obligations, companies could be obligated to disclose the length of time during which manufacturers will provide software patches and updates and connected services to support device functionality.[383] Software patches are integral to data privacy and security. In addition to the data minimization, privacy by default and other recommendations discussed earlier, covered entities could be required to meet detailed privacy and data security standards established by the FTC or other federal agencies for IoT devices.[384]

As I have argued in earlier scholarship, IoT toys and other devices should be designed to function without always having to

---

[382] *See* S. Res. 3586, 2021 Gen. Assembly, Reg. Sess. (N.Y. 2021);); Joshua Mooney, *US Data Privacy Rights Cometh: Multiple States Contemplating Passage of Significant Data Rights Legislation*, KENNEDYS (Oct. 2, 2021), https://kennedyslaw.com/thought-leadership/article/us-data-privacy-rights-cometh-multiple-states-contemplating-passage-of-significant-data-rights-legislation/ [https://perma.cc/2QEA-2FRC] (The "It's Your Data Act," would criminalize (misdemeanor) the collection, storage or use of a person's "name, portrait, picture, video, voice, likeness, and all other personal data, biometric data, and location data" for advertising, trade, data-mining, or generating commercial or economic value without the data subject's consent. It also would criminalize the failure to reasonably protect such data.").

[383] *See, e.g.*, Children and Teens' Online Privacy Protection Act, S. Res 1628, 117th Cong. (2021) ("[A] privacy dashboard under subsection (a) shall inform a consumer of "the minimum length of time during which a connected device will receive security patches and software updates.").

[384] *See id*. At least one scholar has suggested that the FTC should have the power to pursue companies for negligent design of IoT devices that cause harm, but which may not "fall squarely" within the FTC's current framework for unfair and deceptive practices. *Protecting Consumer Privacy, Hearing Before the S. Comm. on Com., Sci. & Transp.*, 117th Cong. 7-8 (2021) (statement of Ashkan Soltani, Independent Technologist).

transmit data and connect to the internet.[385] This proposal could aid in minimizing concerns about rampant data collection and surveillance as well monetization risks that flow from the prevalence of IoT data. It may also help to address civil liberty concerns associated with the disclosure of collected data to governmental entities.

One way to implement this last recommendation is to encourage manufacturers to adopt off switches or "legacy switches" that would render an IoT device "dumb" and disable the features of the device that enable surveillance and privacy harms identified by regulatory agencies, while retaining the normal functionality of a non-IoT device.[386] Thus, for instance an IoT doll could still function as a non-connected doll once the parent or child uses the switch. The off-switch recommendation may work better for some devices rather than others as some devices need internet connectivity and some level of data collection and surveillance to function. While this proposal still involves some level of privacy self-management, it may empower children and parents to limit surveillance more easily.

Lastly, Congress could also consider whether transparency provisions from the EU's Data Act, with necessary adjustments for the U.S. legal landscape, could provide additional benefits for consumers.[387] The EU's Data Act, which entered into force on January 11, 2024, regulates IoT data and establishes "clear and fair rules for accessing and using data," a "necessity heightened by the growing prevalence of the IoT."[388]

---

385 *See, e.g.*, ELVY, A COMMERCIAL LAW OF PRIVACY, *supra* note 55, at 280 (arguing that devices should be able to be designed without such requirements).

386 Paul Ohm & Nathaniel Kim, *Legacy Switches: A Proposal to Protect Privacy, Security, Competition, and the Environment from the Internet of Things*, 84 OHIO ST. L.J. 101, 145 (2023).

387 *See* Regulation 2023/2854, of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), 2023 O.J. (L) 1, https://eur-lex.europa.eu/eli/reg/2023/2854 [https://perma.cc/XLB3-UNYM].

388 European Commission, Shaping Europe's Digital Future (2024), https://digital-strategy.ec.europa.eu/en/node/10725/printable/pdf [https://perma.cc/96HW-XDR2]; *see also* Christopher Foo, *Business to Consumer Impact of the EU Data Act*, ROPES GRAY (Jan. 18, 2024) https://www.ropesgray.com/en/insights/viewpoints/102ix8l/business-to-consumer-impact-of-the-eu-data-act [https://perma.cc/V9YP-TZ5S] ("On 11 January 2024, the EU Data Act entered into force, with the majority of its provisions applicable from 12 September 2025. Among other requirements, the Data Act

IV. CONCLUSION

Increasingly, children's daily activities and experiences both in and outside of their homes are being datafied as companies collect and monetize large quantities "of data points about [children] as they grow up."[389] The IoT and various other technological advancements play an instrumental role in facilitating this datafication. Age-appropriate design mandates in the United Kingdom and California represent an important step towards addressing modern child privacy concerns. However, this area continues to be ripe for legislative intervention in the United States.

---

regulates the access of usage data generated by products connected to the internet (i.e. IoT devices)").

[389] *Executive Summary*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/executive-summary/ [https://perma.cc/BP9J-RS74] (last visited Mar. 19, 2024).