"STITCH" IT TO THE MAN: HOW FASHION BRANDS' TRACKING OF CHILDREN'S CLOTHING IMPLICATES ENFORCEMENT OF COPPA

*Cristina Moga**

INTRODUCTION

Since the invention of Thomas Edison's phonograph and George Eastman's Kodak camera in the late nineteenth century, people have long-desired a shield from being recorded or photographed without their consent.[1] These inventions created a certainty that it was one's right to protect "their beliefs, their thoughts, their emotions and their sensations" that could be captured through these media.[2] Published in 1890 in response to these invasive innovations, Justice Louis Brandeis and Samuel Warren wrote that all individuals have a right "to be let alone" in their private lives.[3] They contended it was important to citizens that they have and retain the power to control what is known about them.[4] Nowadays, developers of smart technology and smart apparel brands unfortunately interfere with a consumer's control over their privacy.[5] It is difficult for a consumer to keep facets of their life private while using smart products because the user has little choice over how their data will be processed. Parents and legal guardians of children have even less choice over how their children's personal data will be treated by smart devices. Thus, the current regulations protecting children's privacy lag behind technological advancements in the smart apparel industry.

Modern application-driven smart devices produced by apparel brands are able to collect more personal data than is necessary for the product's monitoring function.[6] As will be explained, a company that uses this smart technology typically accomplishes this, either intentionally or unintentionally, without the consumer's knowledge or awareness. For example, to distinguish from smart products whose privacy policies transparently convey the types of personal consumer information the seller may access, luxury clothing brand Tommy

* A special thank you to Professor Llewellyn J. Gibbons for his guidance and assistance in writing this Note. Any errors are the fault of the author.

1. Zeynep Tufecki, *We Need to Take Back Our Privacy*, N.Y. TIMES (May 19, 2022), https://www.nytimes.com/2022/05/19/opinion/privacy-technology-data.html.

2. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

3. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

4. *Id.* at 198.

5. Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. MO. BAR 76, 77 (2016).

6. *Id.* at 78.

Hilfiger made it less clear to the purchaser what data its products could access when the company instituted a novel marketing strategy in 2018.[7] Hilfiger launched its Xplore products, each embedded with a Bluetooth smart chip created by Awear Solutions that the consumer could activate, or choose not to activate, with a mobile iOS application ("app").[8] This chip allowed the brand to track how often the buyer wore its products by tracking the wearer's moving location.[9] The wearer could earn loyalty points redeemable for rewards like discounts and tickets to fashion shows.[10] In modern smart products, it is no longer unusual that consumers consent to allow mobile apps to spy on their location, health-based data, or other personal information. Statistics show 85% of Americans now own a smartphone with various apps that track a wide range of personal information.[11]

However, these rapid advancements in technology pose risks to consumers when the law has not caught up with new smart products to properly govern how to limit their access to personal data and offer specific consent. Using Hilfiger's geo-tracking products as an example, what is especially concerning is its lack of transparency demonstrated by its representatives who, when asked, declined to specify "how much personal customer data [was] being collected through the app, or what data [was] provided back to the company."[12] Hilfiger ultimately gave the wearer a choice to inactivate the product's smart chip through the mobile app at any time.[13] But if it was activated, the brand's representatives still refused to "directly address the scope of data collection… beyond acknowledging that there might be personal info."[14] Despite the choice, the wearer had less control over their data than they previously believed if Hilfiger retained or shared data with third parties before the chip's inactivation. Hilfiger's representatives' silence on data access may influence other brands to become lax in their wearer's personal data protection. Apparel brands must follow basic regulations that protect their consumer's data, but these statements show the existing guidelines are not tough enough to ensure the consumer's private information is inviolate. Consumers

---

7. Lisa Lockwood, *Tommy Hilfiger Launches Tommy Jeans Xplore*, WOMEN'S WEAR DAILY (July 25, 2018, 11:37 AM), https://wwd.com/fashion-news/fashion-scoops/tommy-hilfiger-launches-tommy-jeans-xplore-1202764296/.

8. *Id*. (defining "iOS" as an operating system used for mobile devices manufactured by Apple Inc.).

9. *See* Jake Krol, *Tommy Hilfiger's Big Idea for Smart Clothing is to Reward You for Wearing It*, MASHABLE (July 26, 2018), https://mashable.com/article/tommy-jeans-xplore-smart-clothing-rewards-the-wearer. *See generally* Kaylee Fagan, *These $100 Tommy Hilfiger Hoodies Come Equipped with Chips that Track How Often You Wear Them and Give You Prizes*, BUS. INSIDER (July 26, 2018, 6:37 PM), https://www.businessinsider.com/tommy-hilfiger-smart-clothes-rewards-2018-7 (indicating the app contains an exclusive game, comparable to Pokémon Go, where the player earns points by collecting virtual hearts based on their real-world locations).

10. Lockwood, *supra* note 7.

11. *Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/.

12. Fagan, *supra* note 9.

13. Jon Fingas, *Tommy Hilfiger Tracks, Rewards You for Wearing Its Smart Clothes*, ENGADGET (July 26, 2018, 1:57 AM), https://www.engadget.com/2018-07-26-tommy-hilfiger-jeans-xplore.html.

14. *Id.*

should not have to forgo their privacy to partake in whatever is fashionably trending at the moment.

As of September 2023, Hilfiger's Xplore line appears to be unavailable for purchase and the products' corresponding mobile app has been removed from app stores.[15] Yet, apparel brands have already set in motion the next generation of smart clothing. In the fashion industry, there is a concept called the "trickledown" theory of trends where styles that are popularized by top-tier designers, such as Tommy Hilfiger, "trickle down" into the product lines of inexpensive fast fashion brands.[16] This phenomenon makes the styles easily affordable to shoppers who want to dress in the latest trends but often have lower incomes. These affordable brands are mainly marketed towards younger customers, such as young adults, teenagers, tweens, and children, who cannot afford the higher-end brands. Today, this targeted audience has grown up with smart devices and likely will not stop to consider the consequences of sharing personal information with a clothing company's smart products. Hence, amendments to children's privacy laws will help a young consumer make an informed decision about how their data should be processed.

The Children's Online Privacy Protection Act (COPPA) is a U.S. federal privacy law that should be amended to accommodate this fashion trend of embedding smart chips into clothes designed to be worn by children, or consumers under thirteen years of age.[17] Currently, this law requires the consent of both the child and their parent or guardian if a brand's mobile app asks for permission to access a child user's personal data, like geolocation.[18] When given permission, the apparel brand will then be able to track the child's location with the smart chip.[19] However, various past allegations suggest companies may have used the personal information of a minor in violation of COPPA.[20] As will be discussed, the current COPPA regulations are likely unfit to properly govern how companies and brands manage children's data. The Federal Trade Commission ("FTC") is the government agency that enforces this law to protect the privacy and personal data of children.[21] The FTC has the authority to reform COPPA's faulty regulations so

15. *See Tommy Jeans XPLORE*, APPADVICE, https://appadvice.com/app/tommy-jeans-xplore/1393960235 (last visited Aug. 31, 2023). *See generally No Results for Xplore*, TOMMY HILFIGER, https://usa.tommy.com/en/search?search-button=&searchRedirect=true&q=Xplore&lang=en_US&searchterm=null&searchsuggest=null&usertypedsearch=null&previousSearchTerm=null (last visited Aug. 31, 2023) (indicating a word search for "Xplore" brings up "no results").

16. Lloyd A. Fallers, *A Note on the "Trickle Effect,"* 18 PUB. OP. Q. 314, 314 (1954).

17. Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6502 (2023); 16 C.F.R. § 312.2 (2013) (defining "child" as an individual under the age of 13).

18. 15 U.S.C. § 6501 (2023); 16 C.F.R. § 312.2 (2013).

19. Krol, *supra* note 9.

20. *See also* Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 9, United States v. Musical.ly, Inc., No. 2:19-cv-1439 (C.D. Cal. Feb. 27, 2019) (discussing how the platform known as TikTok allegedly illegally collected personal information from children without parental consent but with knowledge children were using its service). *See generally* Complaint at 7-8, In re Retina-X Studios, LLC, No. C-4711 (F.T.C. Mar. 27, 2020) (discussing how the company allegedly failed to secure children's data collected by its "stalking" apps and ensure the apps were used for legitimate purposes).

21. 16 C.F.R. § 312 (2013).

they may successfully govern the smart apparel industry's technology. These regulations include a child's geolocation tracking, a brand's "actual knowledge" requirement of serving a child audience, and whether a child's data is used for a fair purpose of locating a child or for an exploitative marketing purpose.[22]

Enacted in 1998, COPPA is far too outdated to regulate modern smart devices because it was introduced years before children could possess smartphones.[23] COPPA's data tracking regulations are underdeveloped and cannot properly govern the nascent trend of tracking an article of clothing and its wearer. This Note will analyze COPPA's outdated geolocation tracking, actual knowledge requirement, and fair purposes for data use regulations in relation to children's smart apparel. A proposed solution is as follows: amend COPPA to offer parents of child users the ability to consent to a company's use of the child's geolocation information *without* consenting to using the data for direct marketing purposes. This solution will hopefully initiate a trend wherein companies offer the user an opportunity to customize how their data will be processed via an easy-to-use settings dashboard on their smart device. Further, an extension of COPPA's data privacy protection to privacy laws governing adult consumers would allow users of all ages to make an informed decision to opt in or out of certain data collecting practices while maintaining the ability to use the device for its full function.

Part I discusses the importance of a parent's right to control their child's privacy under COPPA following this rise in smart technology. Part II introduces how COPPA has been applied to relevant modern cases as the FTC continues to bring new charges against mobile app-creators every year. Part III addresses COPPA's regulations and their issues pertinent to the smart apparel industry. Finally, Part IV proposes a solution to reform COPPA's geolocation data tracking regulations. A new COPPA regulation should instruct companies to give users a choice to consent to precise location data and, at the same time, opt out of geo-targeted marketing in preparation for this trend of children's clothing embedded with trackable smart chips.

I. DRAFTING: PRIVACY FOR THE WHOLE FAMILY

An individual's right to privacy was established as a fundamental human right by the Supreme Court when it held that the Bill of Rights confers upon individuals an implied right to privacy.[24] Although the U.S. Constitution does not explicitly guarantee a right to privacy, people value privacy for their own safety.[25] A right to privacy is assumed because it is natural for a person to keep aspects of

22. *See* 16 C.F.R. § 312.2 (2013).

23. *General Questions About the COPPA Rule*, Section A(1) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section A(1)*].

24. Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

25. *See id.* at 483-85 (describing that an implied right to privacy is derived from "penumbras" of other explicitly stated constitutional protections found in the First, Third, Fourth, Fifth, and Ninth Amendments); Michael Froomkin & Zak Colangelo, *Privacy as Safety*, 95 WASH. L. REV. 141, 163 (2020) (discussing several ways privacy enhances safety).

their personal life unshared with others by choice. COPPA confirms these notions by bestowing upon parents a right to consent on their child's behalf to protect the child's safety as well as the family's personal information that could be passed on from the child to abusive entities.[26]

COPPA's language teaches citizens that their identifiable data includes a person's full name, date of birth, phone number, geolocation coordinates, email, home and IP addresses, credit or debit card numbers or banking information, and Social Security Number.[27] Citizens should be wary that this valuable information stored on smart devices may be so easily accessed by private entities with few repercussions. Notably, a collective accumulation of personal data that a company may possess poses harmful risks to the consumer. Data aggregation, often achieved by data brokers and their sale of personal data, can be more harmful than if a company were to collect individual pieces of data which would help keep the user anonymous.[28] Cyber fraud, like identity theft, concerns consumers whose data is stored indefinitely.[29] Even if the consumer willingly consents only to momentary data collection, individual instances of data aggregation could be added up and strung together to reveal a consumer's identity.[30] Thus, COPPA advises companies to retain children's data only to the extent reasonably necessary for the function of their service rather than storing data indefinitely.[31] For instance, if geolocation tracking may be selectively turned off, the consumer is only "stopping the app from using one particular kind of ID that exists" within the product while still allowing other data to be collected to possibly identify the user.[32] This suggests that simply pausing the collection of a specific type of data does not automatically erase the data that has already been collected. A company's access to so much retained data about a child, let alone any adult user, may harm the child's online safety.

With the rise of the internet, parental concern increased for their children who could easily publish inordinate amounts of their own personal information online where predatory practices over children could be exercised by others.[33] Congress passed COPPA to ensure children's safety by permitting parents to control what information children share.[34] COPPA imposes requirements on the operators of websites and online services that produce mobile device apps directed to

---

26. 16 C.F.R. § 312.5(a) (2013).

27. 15 U.S.C. § 6501 (2023); 16 C.F.R. § 312.2 (2013).

28. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY v-vii 3 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; Clare Cho & Kristen Busch, ONLINE CONSUMER DATA COLLECTION 2-4 (Oct. 31, 2022), https://sgp.fas.org/crs/misc/R47298.pdf.

29. DATA BROKERS, *supra* note 28, at vi.

30. Cho & Busch, *supra* note 28, at 3-4.

31. 15 U.S.C. § 6502 (2023); 16 C.F.R. § 312.10 (2013).

32. Dave Davies, *Users Beware: Apps are Using a Loophole in Privacy Law to Track Kids' Phones*, NPR (June 16, 2022, 12:38 PM), https://www.npr.org/2022/06/16/1105212701/users-beware-apps-are-using-a-loophole-in-privacy-law-to-track-kids-phones.

33. Melanie L. Hersh, *Is COPPA a Cop Out - The Child Online Privacy Protection Act as Proof that Parents, Not Government, Should Be Protecting Children's Interests on the Internet*, 28 FORDHAM URB. L. J. 1831, 1833 (2001).

34. *See Complying with COPPA Section A(1)*, *supra* note 23.

children.[35] These requirements generally prohibit companies from either actively or passively collecting a child's personal data without parental consent if the company has actual knowledge they collected data from a child user.[36] Parents should be aware of how and to what extent their child's personal data, like precise geolocation data, is being garnered through apps in order to protect their child's safety and well-being.

Although children retain basic human rights, parents have an established right to control the care and wellbeing of their children.[37] It is important for parents to be placed in control of their child's online access privileges on smart products because of the harms to which children could be exposed. The FTC recognizes that children are "particularly vulnerable to overreaching by marketers and may not understand the safety and privacy issues created" by data collection.[38] Children can be easily influenced by content they see online and may not be able to make mature decisions.[39]

The COVID-19 pandemic triggered children at home to increase their screen time.[40] Parents are justified in their concerns for their child's online exposure to groomers, cyberbullying, depression, substance use, interactions with strangers, and body image misperceptions that may lead to eating disorders.[41] Exposure may lead to further and more severe victimization, like child abduction, and the survivor may struggle later in life with personal relationships from the effects of their experience.[42] Online parental controls help parents protect their children from interacting with online strangers, seeing age-inappropriate content, or being subjected to child predation and data practices that commercialize children's data.

---

35. 15 U.S.C. § 6502 (2023); 16 C.F.R. § 312.3 (2013).

36. *Id.*

37. Troxel v. Granville, 530 U.S. 57, 66 (2000); Pierce v. Soc'y of Sisters, 268 U.S. 510, 534-35 (1925).

38. *General Questions About the COPPA Rule,* Section A(9) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section A(9)*].

39. *Constantly Connected: How Media Use Can Affect Your Child*, HEALTHY CHILD., https://www.healthychildren.org/English/family-life/Media/Pages/adverse-effects-of-television-commercials.aspx (last updated Mar. 30, 2023) (citing substance use, sexting, and presence of online predators as reasons to limit children's media use).

40. *The Common Sense Census: Media Use by Tweens and Teens, 2021,* COMMON SENSE MEDIA, (Mar. 9, 2022), https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens-2021 (showing media use by tweens and teens rose faster in the two years since the COVID-19 pandemic than the four years before).

41. Elena Bozzola et al., *The Use of Social Media in Children and Adolescents: Scoping Review on the Potential Risks*, 19 INT'L J. ENV'T RSCH. PUB. HEALTH 11 (2022), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9407706/ (mentioning adult marketing and a strong advertising presence on social media sites).

42. Alicia Kozakiewicz, *Kidnapped by a Paedophile I Met Online*, BBC NEWS (Mar. 7, 2016), https://www.bbc.com/news/magazine-35730298 (recounting an early instance in 2002 when a teen was lured and kidnapped by someone she met in an online chat room); Tina Burnside, *Missing Dallas Teen Found Locked in a Shed Was Abducted and Raped by Man She Met Online, Authorities Say*, CNN (Mar. 14, 2023, 12:59 PM), https://www.cnn.com/2023/03/14/us/north-carolina-missing-teen-dallas-found/index.html.

In the context of smart apparel, brands that track a child consumer's geolocation for a point-earning rewards system place profits over the child's safety.

A. The Rise in New Smart Technology Will Increase Chances of Data Privacy Violations

Today, companies must navigate collecting certain types of data depending on the function of their product or service without infringing upon the consumer's right to privacy. In particular, the development of smart devices in the clothing industry is a legal area where companies must be particularly careful because these products can collect an immense amount of data from a single consumer.

At the beginning of the smart apparel era, the introduction of wearable devices and smart clothing into the health and fitness apparel industry began with at least one specific goal in mind: to improve the wearer's lifestyle.[43] Sensoria, Fitbit, and other apparel brands sell smart garments containing biometric-monitoring technology that tracks and collects the wearer's physiological information.[44] Such technology can monitor factors like body temperature, external environmental conditions, heart rate, and diet behaviors.[45] Once the wearer receives feedback that is reviewable through an app downloaded onto the owner's mobile device, they can adjust their actions accordingly to enhance their wellness.[46] For example, parents may purchase Owlet's smart "Dream Sock" for their newborn babies and toddlers which tracks physiology including oxygen levels and heart rate.[47]

The collective allegations brought by the United States and the FTC against Facebook, the social networking platform, provide a first look into possibly major privacy violations by the industry giant.[48] In *United States v. Facebook*, Facebook allegedly failed to improve its privacy settings to address third party manipulation despite having been presented in 2012 an FTC order to do so.[49] In *In the Matter of Facebook, Inc.* of 2012, the FTC alleged that the platform misrepresented how its users could control their private data through Facebook's privacy settings.[50] At that time, third party app developers were believed to have accessed most of a user's personal data, including birthdates and place of employment, if the user installed

---

43. Simone Benatti et al., *Towards EMG Control Interface for Smart Garments*, ISWC 163-64 (2014), https://dl.acm.org/doi/abs/10.1145/2641248.2641352.

44. Shourjya Sanyal, *Are Smart Biometric Garments Going to Replace My Family Doctor?*, FORBES (Jan. 28, 2019, 7:47 AM), https://www.forbes.com/sites/shourjyasanyal/2019/01/28/are-smart-biometric-garments-going-to-replace-my-family-doctor/?sh=459e546a54d7.

45. Sumin Helen Koo & Kristopher Fallon, *Explorations of Wearable Technology for Tracking Self and Others*, FASHION TEXTILES 5, 8 (2018), https://fashionandtextiles.springeropen.com/articles/10.1186/s40691-017-0123-z.

46. *Id.* at 3.

47. *13 Best Smart Clothing for Performance and Health*, FIBRE2FASHION, https://www.fibre2fashion.com/industry-article/8983/13-best-smart-clothing-for-performance-and-health-2021-update (last visited Feb. 11, 2023).

48. *See* Complaint for Civil Penalties, Injunction, and Other Relief, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. July 24, 2019) [hereinafter *2019 Facebook Complaint*].

49. *Id.* at 3-4.

50. Complaint at 6-9, In the Matter of Facebook, Inc., No. C-4365 (F.T.C. Aug. 10, 2012).

their app even though Facebook assured users they could control who could see their profile information.[51] In the subsequent settlement, Facebook was ordered to give users clear notice in its privacy settings concerning who can access their personal information.[52] Over several years, Facebook supposedly ignored its obligations to respect its user's personal information by allowing third parties to steal the private data of users.[53]

Facebook sparked national concern for user privacy when a whistleblower admitted in 2018 that a third party political advertiser, Cambridge Analytica, had accessed millions of users' sensitive information without the user's express consent.[54] This occurred despite the fact that users were allegedly assured their personally identifiable data would be secure.[55] Through a sneaky process, users unknowingly granted permission for the third-party to access their friends' profiles when they filled out a seemingly harmless personality test assumed to be used for research purposes only.[56] The personal data harvested from these pages was used to create a system that would profile voters and target them with personalized political ads in anticipation of the upcoming U.S. Presidential election.[57] The FTC declared Cambridge Analytica's several years of mistreatment and collection of user data a violation of consumer privacy law.[58]

Later, Facebook's questionable security methods would lead to a data breach of nearly fifty million accounts.[59] After these incidents, Facebook settled with the FTC to pay a five billion dollar fine and was ordered to "exercise greater oversight over third-party apps, including by terminating app developers that fail to certify that they are in compliance with Facebook's platform policies[.]"[60] Again, Facebook was ordered to establish mechanisms that boosted the transparency of a user's privacy decisions, but the damage to eighty-seven million Facebook users

---

51. *Id.* at 6.

52. *FTC Approves Final Settlement with Facebook*, FED. TRADE COMM'N (Aug. 10, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/08/ftc-approves-final-settlement-facebook.

53. *2019 Facebook Complaint*, *supra* note 48, at 3-5.

54. Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, THE GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

55. *FTC Sues Cambridge Analytica, Settles with Former CEO and App Developer*, FED. TRADE COMM'N (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer.

56. Cadwalladr & Graham-Harrison, *supra* note 54.

57. *Id.*

58. Opinion of the Commission at 2-3, In the Matter of Cambridge Analytica, LLC, No. 9383 (F.T.C. Nov. 25, 2019).

59. Julia Carrie Wong, *Facebook Says Nearly 50m Users Compromised in Huge Security Breach*, THE GUARDIAN (Sept. 28, 2018), https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach.

60. *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

had already been done.[61] Regardless of court orders to restructure its privacy policy, Facebook's repeat offenses as a major social media platform weakened the FTC's credibility because of its apparent inability to keep an online user's personal data secure from unlawful exposure. Just as "Facebook's innovation [did] not have to come at the expense of consumer privacy,"[62] consumers of smart apparel should not have to exchange valuable personal information, such as geolocation coordinates, for very little in return, like rewards points, at the possible risk of having their data impermissibly sold or disseminated.[63]

II. TRACING: FTC ENFORCEMENT PATTERNS IN RECENT COPPA CASES

The FTC was created pursuant to the Federal Trade Commission Act of 1914 to focus on combatting consumer protection violations and by outlawing unfair or deceptive commercial business practices that affect American consumers.[64] Congress has granted the FTC greater authority to police companies and bring them into compliance with privacy laws by imposing severe civil punishments and often pursuing court orders to change unlawful business methods.[65] While promoting honest competition, this federal agency also endeavors to protect the consumer's privacy and data security from entities that have violated COPPA regulations.[66] Parents can report their suspicions to FTC staffers so that the FTC may bring civil penalties for potentially over fifty-thousand dollars per violation if it has reason to believe the entity violated or is about to violate COPPA.[67]

The FTC enforces COPPA violations because they are considered unfair and deceptive trade practices.[68] This is one of the few U.S. privacy laws that functions to protect children's data from exploitation. Under this law, app-driven companies must provide child users and their parents with a clear privacy policy, obtain verifiable parental consent ("VPC") to access a child's data, keep that data properly

61. Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief at 5-8, United States v. Facebook, Inc., No. 19-cv-2184 (D.C.C. July 24, 2019) (implementing solutions to overhaul the way Facebook makes privacy decisions).

62. *Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises*, FED. TRADE COMM'N (Nov. 29, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises.

63. *See generally* Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 11-12, United States v. Kuuhuub, Inc., No. 1:21-cv-01758 (D.D.C. June 30, 2021) (stating that an online coloring book app directed at a mixed audience allegedly offered users social media features in exchange for collecting children's personal information without parental consent).

64. 16 C.F.R. §§ 0.1, 0.17 (2013).

65. 15 U.S.C. § 45(l) (2023).

66. 15 U.S.C. § 6502(a)-(c) (2023).

67. *COPPA Enforcement*, Section B(1) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#B.%20COPPA%20Enforcement (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section B(1)*]; *COPPA Enforcement*, Section B(2) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#B.%20COPPA%20Enforcement (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section B(2)*].

68. 15 C.F.R. § 6502(b)(1) (2023).

secure, and delete the data automatically after it has fulfilled its purpose.[69] Outside of the U.S., foreign companies must also comply with COPPA if their services are directed to children in the U.S.[70]

There are exceptions, of course, to evading parental consent, but they are usually in the context of a "one-time basis" with the child user.[71] For instance, operators may obtain a child user's contact information to notify them only in the event they win a prize from a contest.[72] Operators are instructed to erase all contact information they obtained after a certain time period rather than store it.[73] For the "multiple online communications" exception to apply, a company must obtain the parent's contact information and offer them the opportunity to opt out if the child's data is typically retained.[74] These exceptions still prohibit the company from using the child's data for any other purpose.[75] A company must not retain a child's data for longer than is reasonably necessary, meaning the company may retain data either for as long as needed for the child to participate in the service or for the purpose of supporting the company's "internal operations" which allow the application to function.[76] Further, VPC is required if companies ask for more data than is necessary.[77]

The FTC offers a non-exhaustive list of suggestions on how companies may acquire VPC.[78] This includes the parent signing a mailed form, submitting their driver's license number or Social Security Number for processing, or making a nominal monetary transaction via credit or debit card.[79] However, these methods may waste time or seem inconvenient for some parents. Other parents may not be in a position to satisfy a particular VPC option that a company requires, such as producing a government I.D. or bank account information. The effectiveness of these options is also questionable because a parent could be impersonated by someone without a familial relationship to the child. Most importantly, parents would understandably be concerned about producing their own personal information and passing it on to these unknown companies.

There are two other caveats to COPPA's regulatory language concerning the intended audience of an operator's mobile device app. First, a company is required to obtain parental consent to data access if the service is child-directed.[80] A balancing factor test is used to determine whether a company's service is child-directed.[81] These factors, which include subject matter, visual content, use of animated characters or child-oriented activities or characteristics, age of models,

69. 15 U.S.C. §§ 6501-6502 (a)(i)-(ii) (2023); 16 C.F.R. §§ 312.10, 312.8 (2013).
70. 15 U.S.C. § 45(a)(4)(A) (2023); 16 C.F.R. § 312.2 (2023).
71. 15 U.S.C. § 6502(b)(2) (2023); 16 C.F.R. § 312.5(c)(3) (2013).
72. 15 U.S.C. § 6502(b)(1)(C) (2023); 16 C.F.R. §§ 312.7, 312.5(c)(3) (2013).
73. 15 U.S.C. § 6502(b)(2)(A) (2023); 16 C.F.R. § 312.5(c)(3) (2013).
74. 15 U.S.C. § 6502(b)(2)(C) (2023); 16 C.F.R. § 312.4(c)(3) (2013).
75. 15 U.S.C. § 6502 (b)(2)(A)-(C) (2023).
76. 15 U.S.C. §§ 6501(4)(A), 6502(b)(2)(E)(i) (2023); 16 C.F.R. § 312.10 (2013).
77. 15 U.S.C. §§ 6501(a), 6502(b)(1)(A)(ii) (2023); 16 C.F.R. § 312.5 (a)(1) (2013).
78. 16 C.F.R. § 312.5(b)(2) (2013).
79. *Id.*
80. 15 U.S.C. § 6502(b)(1) (2023).
81. 15 U.S.C. § 6501(10)(A) (2023); 16 C.F.R. § 312.2 (2013).

presence of child celebrities, language, and audience composition, are to be weighed to determine the operator's intended audience.[82] The FTC applies the totality of the circumstances to determine if a service is child-directed despite the operator's alleged intent.[83] For instance, mobile applications involving activities that have been traditionally reserved for adults, like financing and home improvement, are clearly not intended for children. However, as will be discussed later, it is not always clear if the service is child-directed based on its content.

Operators of child-directed services are not usually permitted to age-screen visitors since all visitors are considered children, but services directed at a "mixed audience" may implement an age screening process.[84] This audience is another category of child-directed services where children are not the primary audience, though they are an intended portion of viewers along with adults or older teenagers.[85] When targeting a "mixed audience," operators may screen a visitor's age as long as they have not collected personal information before they verify their age via an age-neutral screening mechanism that permits a visitor to freely enter their month and year of birth.[86] To be a neutral mechanism, the operator should avoid warning visitors that children may not use their services as this could encourage children to falsify their age.[87] The FTC suggests that companies should

---

82. 16 C.F.R. §312.2 (2013). *See generally* Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 6, United States v. TinyCo, Inc., No.:3:14-cv-04164 (N.D. Cal. Sept. 16, 2014) (discussing how mobile app allegedly targeted children with themes appealing to children, brightly colored animated characters, and simple language); Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 10-11, United States v. Hyperbeard, Inc., No.: 3:20-cv-3683 (N.D. Cal. June 3, 2020) (discussing how mobile app developer allegedly had actual knowledge children used its service by promoting its app on kids' entertainment websites, publishing children's books, and licensing stuffed animals).

83. *General Audience and Teen Sites or Services,* Section H(5) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#H.%20General%20Audience%20and%20Teen%20SIte s (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section H(5)*].

84. *Websites and Online Services Directed to Children, Including Mixed Audience Sites and Services,* Section D(4) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#D.%20Websites%20and%20Online%20Services (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section D(4)*]; *Websites and Online Services Directed to Children, Including Mixed Audience Sites and Services,* Section D(6) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#D.%20Websites%20and%20Online%20Services (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section D(6)*].

85. *Complying with COPPA Section D(4)*, *supra* note 84; *Complying with COPPA Section H(5)*, *supra* note 83.

86. *Complying with COPPA Section D(4)*, *supra* note 84; *Websites and Online Services Directed to Children, Including Mixed Audience Sites and Services,* Section D(7) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#D.%20Websites%20and%20Online%20Services (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section D(7)*].

87. *General Audience and Teen Sites or Services,* Section H(3) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#H.%20General%20Audience%20and%20Teen%20SIte s (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section H(3)*]; *see generally* Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief at 8-9, United States

use a single persistent identifier, like a cookie, in this case to prevent children from back-buttoning to enter a different age.[88] However, this will not block children from using these services and their profiles will only be differentiated from other users over the age of consent.[89] The company will know not to collect data from visitors that identify as under thirteen years of age.

The second caveat concerns services directed towards "general audiences," or users of all ages.[90] Although companies that direct its services to everyone are not required to investigate a visitor's age through an age screen, they have discretion to block child visitors from using the services with an age screen.[91] Here, a company is only liable for violating COPPA when it has "actual knowledge" that it collected data from a minor user without parental consent.[92] For example, a company may be deemed to have knowledge if the child leaves a public comment stating they are in middle school. This "actual knowledge" requirement also applies to operators that know third parties have collected children's data from their service.[93] The only standard a general audience operator must follow once they have actual knowledge of collecting data from child users is to either obtain VPC or delete the child's data.[94]

---

v. Kurbo, Inc., No. 22-CV-946 (N.D. Cal. Feb. 16, 2022) (discussing how this company's signup process allegedly permitted an underage user to falsify their age—if a minor truthfully changed their age, they could still access the mobile application's features).

88. *Complying with COPPA Section D(7), supra* note 86.

89. *Complying with COPPA Section D(6), supra* note 84.

90. *Complying with COPPA Section D(4), supra* note 84.

91. *General Audience and Teen Sites or Services,* Section H(1) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#H.%20General%20Audience%20and%20Teen%20SItes (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section H(1)*]. *See also Complying with COPPA Section H(3), supra* note 87.

92. 15 U.S.C. § 6502(a)(1) (2023); 16 C.F.R. § 312.3 (2013). *See generally* Complaint for Permanent Injunction, Civil Penalties and Other Relief at 6-7, United States v. Yelp Inc., No.: 3:14-cv-04163 (N.D. Cal. Sept. 16, 2014) (discussing how this mobile app allegedly failed to implement an adequate age-screen and collected personal information from children without parental consent even when it obtained actual knowledge of registrants' birth dates).

93. *Third Parties, Such as Ad Networks and Plug-Ins, Collecting Personal Information on Sites Directed to Children,* Section E(1) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#E.%20Third%20Parties (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section E(1)*]; *Disclosure of Information to Third Parties,* Section L(1) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#E.%20Third%20Parties (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section L(1)*];

94. *General Audience and Teen Sites or Services,* Section H(4) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#H.%20General%20Audience%20and%20Teen%20SItes (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section H(4)*]; *General Audience and Teen Sites or Services,* Section H(6) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#H.%20General%20Audience%20and%20Teen%20SItes (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section H(6)*].

The three cases discussed below demonstrate how the FTC has generally applied COPPA to alleged privacy violations. The settled cases display how the FTC deals with the child-directed factors as well as actual knowledge. It may break the reader's trust in privacy laws to see how easily companies can take advantage of their users.

In the two and a half decades of COPPA's existence, the FTC has sought civil fines in the millions of dollars against companies accused of violating COPPA.[95] In 2022, the FTC settled a case against Epic Games, Inc., the creator of the popular video game Fortnite, collecting a record monetary penalty of $520,000,000 for allegedly violating COPPA.[96] In *United States v. Epic Games, Inc.*, Epic allegedly engaged in unfair practices by imposing real-time communications through an on-by-default voice and text chat privacy control setting without notifying a minor child's parents, obtaining parental consent, or allowing players to easily turn the setting off for privacy.[97] This live gameplay setting supposedly allowed all players, regardless of their age, or even after they identified themselves as a child, to automatically and publicly broadcast their name to facilitate conversations with online strangers.[98] First, the FTC alleged that the creators directed this free network-connected game to children by taking into consideration "surveys of Fortnite users, the licensing and marketing of Fortnite toys and merchandise, player support and other company communications[.]"[99] These factors implied that the makers had actual knowledge that children played their online game. Second, Epic allegedly failed to honor parental requests to have their child's personal information deleted after parents attempted to jump through unreasonable hoops for data review and erasure.[100] Fortnite's allegedly unfair default settings enraged parents when the automatically-enabled, real-time chat settings supposedly matched child and teen players with online strangers and publicly broadcasted the player's account names.[101] This allegedly exposed the minor player to harmful bullying, threats, and sexual harassment.[102] The FTC now uniquely requires Epic to implement stronger, easy to locate privacy settings by having these communications turned off by default to protect a child user from harmful verbal

95. *See History of COPPA & GDPR Violations*, PRIVO, https://www.privo.com/history-of-coppa-gdpr-violations (last updated June 5, 2023) (presenting a historical timeline of alleged COPPA violations and fines dating back to 1999).

96. *Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars Over FTC Allegations of Privacy Violations and Unwanted Charges*, FED. TRADE COMM'N (Dec. 19, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations [hereinafter *Epic Games Press Release*].

97. Complaint for Permanent Injunction, Civil Penalties, and Other Relief at 22-23, 28-30, United States v. Epic Games, Inc., No. 5:22-C-00518 (E.D.N.C. Dec. 19, 2022) [hereinafter *Epic Games Complaint*].

98. *Id.* at 26, 30.

99. *Epic Games Press Release*, *supra* note 96.

100. *Epic Games Complaint*, *supra* note 97, at 23, 28-29.

101. *Id.* at 16-19.

102. *Id.* at 18.

content.[103] Unless the child falsifies their age, the new opt-in default privacy setting may be switched off only with a parent's affirmative consent.[104]

Similarly, allegations for COPPA violations against Google and its subsidiary YouTube demonstrate that interactions with prospective corporate clients, advertising companies, and internal content rating systems may all serve as relevant factors in determining "actual knowledge" of child users.[105] In *FTC v. Google, LLC*, child-directed YouTube channels allegedly collected children's personal information illegally without parental consent by using numerous persistent identifiers that tracked users across the internet.[106] In violation of COPPA, children's data was supposedly collected even when YouTube's content rating system identified a channel's content to be child-directed.[107] YouTube then allegedly profited from delivering targeted ads to viewers of these channels based on the users' internet browsing habits.[108] Although children may still misstate their age to bypass the age-gate required to make a YouTube "main" account, YouTube Kids, the child-targeted version of YouTube, protects children's personal data by prohibiting features like behavioral, or "interest-based" advertising.[109] The FTC argued that YouTube had actual knowledge of collecting children's data when YouTube bragged about "market[ing] itself as a top destination for kids in presentations to the makers of popular children's products and brands" in relation to its child users' preference for the video sharing site over top television shows.[110] With a substantial fine, the FTC ordered YouTube to enhance its child-directed content identification system and instruct content creators to make a "clear and conspicuous" disclosure to viewers that their channel's content was directed at children.[111]

In *United States v. OpenX Technologies, Inc.*, an online advertising auction-like platform allegedly violated COPPA for collecting personal information from children without parental consent.[112] To sell targeted ad space for websites and mobile apps, OpenX would have an obligation to flag mobile apps intended for children so that the child user's collected personal information would remain

---

103. Stipulated Order for Permanent Injunction and Civil Penalty Judgment at 17-19, United States v. Epic Games, Inc., No. 5:22-CV-00518-BO (E.D.N.C. Dec. 19, 2022).

104. *Epic Games Press Release*, *supra* note 96.

105. Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief at 8-9, 15, FTC v. Google, Inc., No.1:19-cv-02642 (D.D.C. Sept. 4, 2019); *See* Revised Exhibits A-C, FTC v. Google, Inc., No. 1:19-cv-02642 (D.D.C. Sept. 6, 2019).

106. *Id.* at 15-16.

107. *Id.*

108. *Id.* at 7, 14-15.

109. *Advertising on YouTube Kids*, GOOGLE SUPPORT, https://support.google.com/youtube/answer/6168681?hl=en (last visited Sept. 1, 2023).

110. *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, FED. TRADE COMM'N (Sept. 4, 2019), https://www.ftc.gov/news-events/pressreleases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

111. Stipulated Order for Permanent Injunction and Civil Penalty Judgment at 10-11, 13, FTC v. Google, LLC, No.: 1:19-cv-02642 (D.C.C. Sept. 10, 2019).

112. Complaint for Permanent Injunction, Civil Penalties, and Other Relief at 13-14, United States v. OpenX Technologies, Inc., No: 2:21-cv-09693 (C.D. Cal. Dec. 15, 2021) [hereinafter *OpenX Complaint*].

unshared in the company's bidding ad exchange.[113] However, some child-directed apps that were not properly flagged allegedly participated in the exchange, so a child user's personal data was passed on to third parties that used the data to target children with unique ads on their mobile apps.[114] The platform was ordered to comply with COPPA and cease collecting children's personal data by revising how it identified child-directed mobile apps.[115] What is most concerning about this case is that OpenX may have secretly collected precise geolocation data from mobile users who explicitly asked not to have their location tracked by opting out of this type of data collection.[116]

This selection of cases demonstrates that companies may remain capable of circumventing privacy laws by exposing a child's private information to malicious use twenty-five years after COPPA was enacted. These cases were all brought after the collection of data had already supposedly been compromised and used to the company's benefit. The likely mistreatment of consumer data calls into question the effectiveness of COPPA's existing regulations and their enforcement by the FTC. COPPA in its current form cannot properly protect private consumer information in connection with the smart apparel they wear, especially if future children's smart apparel manufacturers become prone to privacy breaches.

III. ALTERING: COPPA'S REGULATIONS ARE NOT ON-BRAND FOR SMART APPAREL

There is evidence that COPPA's regulations are not equipped to govern child-directed ads, the knowing collection of children's data, or, in particular, the geolocation of clothing in our modern marketplace. In 2013, COPPA was broadened to include coverage of an entity's unlawful use, collection, or sharing of geolocation data.[117] Geolocation data that is sufficient to identify a street name or the name of a city or town qualifies as individually identifiable information.[118] Even if not used for the service's functional purpose, the company still must place parents on notice and give them a choice to consent to the company collecting their child's location data.[119] For example, the 2013 amendment broadened personal data to a company's implementation of "persistent identifiers" that can recognize and passively track users over time via geolocation or GPS.[120] These identifiers

113. *Id*. at 9-11.

114. *Id.* at 10-11.

115. Stipulated Order for Permanent Injunction and Civil Penalty Judgment at 8, 11, United States v. OpenX Technologies, Inc., No.: 2:21-cv-09693 (C.D. Cal. Dec. 15, 2021) [hereinafter *OpenX Stipulated Order*].

116. *OpenX Complaint*, *supra* note 112, at 8, 12. *See OpenX Stipulated Order*, *supra* note 115, at 9 (presenting the injunction requiring user consent for collection of location information).

117. *Revised Children's Online Privacy Protection Rule Goes into Effect Today*, FED. TRADE COMM'N (July 1, 2013), https://www.ftc.gov/news-events/news/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect-today [hereinafter *Revised COPPA Press Release*].

118. 15 U.S.C. § 6501(8)(b) (2023); 16 C.F.R. § 312.2 (2013).

119. 16 C.F.R. § 312.4(a) (2013).

120. *Revised COPPA Press Release*, *supra* note 117.

include a consumer's recognizable number within a "cookie, an [IP] address, a processor or device serial number, [a] unique device identifier," or a globally unique identifier.[121] This is one way for companies to deliver personalized content to a user in the form of ads—by following a user's shopping history or prior travel habits. Algorithms may keep track of a user's interests via search engine plugins so that marketers may provide the user with custom-located information or goods based on purchasing history in the user's local area.

As previously alluded to, the exception to the collection of persistent identifiers without parental notice or consent is typically permitted only if the data was collected for the sole purpose of providing "support for the internal operations."[122] Then, companies may track and retain persistent identifiers only for the service to function properly, which includes personalization that maintains the user's interface preferences.[123] Persistent identifiers should not be amassed to identify a user or disclose a user's personal information to third parties for exploitative reasons, like behavioral advertising.[124] Without giving notice or obtaining parental consent, companies and their affiliated third parties may use persistent identifiers for contextual advertising that is related to the service's own content rather than targeted ads.[125] The operator is responsible for the actions of the third party and must confirm that the third party's information collection practices comply with COPPA.[126]

Similar to the question of geolocation tracking in *OpenX*, InMobi also allegedly violated COPPA's requirement for consent of geolocation tracking.[127] In *United States v. InMobi Pte Ltd*, a mobile advertising network was alleged to have deceptively tracked consumer's geolocations without their knowledge, including

---

121. 16 C.F.R. § 312.2 (2013).

122. 16 C.F.R. § 312.5(c)(7) (2013).

123. *Exceptions to Prior Parental Consent*, Section J(8) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#J.%20Exceptions%20to%20Prior%20Parental%20Consent (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section J(8)*] (presenting that the FTC outlines other necessary functions, but they are beyond the scope of this paper).

124. *Exceptions to Prior Parental Consent*, Section J(5) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#J.%20Exceptions%20to%20Prior%20Parental%20Consent (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section J(5)*].

125. *Complying with COPPA Section J(5)*, *supra* note 124; *Complying with COPPA Section J(8)*, *supra* note 123.

126. *Complying with COPPA Section L(1)*, *supra* note 93; *Websites and Online Services Directed to Children, Including Mixed Audience Sites and Services*, Section D(9) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#D.%20Websites%20and%20Online%20Services (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section D(9)*]; *Websites and Online Services Directed to Children, Including Mixed Audience Sites and Services*, Section D(11) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#D.%20Websites%20and%20Online%20Services (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section D(11)*].

127. Complaint for Permanent Injunction, Civil Penalties and Other Relief at 12-14, United States v. InMobi Pte Ltd., No. 3:16-cv-3474 (N.D. Cal. June 22, 2016) [hereinafter *InMobi Complaint*].

children's locations without parental permission.[128] The company allegedly tracked a consumer's location to serve them geo-targeted advertising by combining geolocation data with wireless networks near consumers to infer a consumer's precise location.[129] The ads were often supposedly served to a consumer based on their current location, locations they had visited, or their location over time.[130] The software allegedly continued to track geolocation even after a user denied it permission to access this data or regardless of whether the consumer had provided opt-in consent.[131] Notably, these are the few companies that happened to get caught violating COPPA. This pattern of companies finding new ways to evade children's privacy laws is likely to continue if children's clothing is embedded with location-tracking chips.

A. Offering Customized Consent to Geolocation-Tracking Clothes for All Ages

There is a strong incentive to recycle COPPA's parental consent requirement regarding geolocation tracking for children and to integrate the concept into *all* consumer data privacy laws that govern wearable smart devices and new smart leisure apparel. Precise geolocation tracking may be especially harmful to the wearer if a company leaks to a third party the exact places the wearer visits.[132] For instance, the FTC filed a pivotal lawsuit against Kochava, Inc., a data broker company that allegedly sold timestamped geolocation data from its users' mobile devices.[133] In *FTC v. Kochava, Inc.*, it was alleged that the company could trace a user's movements to sensitive locations like reproductive health clinics, places of worship, homeless and domestic violence shelters, or addiction recovery facilities.[134] By supposedly selling a user's accumulation of personal data to an outside party, the information could be used to identify the user and expose them to threats of stigma, stalking, discrimination, job loss, and physical violence.[135] Although this case was recently dismissed, the FTC was given the opportunity to

128. *Id.* at 3, 12-14.

129. *Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission*, FED. TRADE COMM'N (June 22, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked-hundreds-millions-consumers.

130. *Id.*

131. *InMobi Complaint*, *supra* note 127, at 9, 13.

132. *AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities*, COMMONWEALTH OF MA (Apr. 4, 2017), https://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts-healthcare-facilities (explaining a company allegedly violated state consumer protection laws when it used mobile geofencing to direct third-party pro-birth advertising to women in reproductive health facilities).

133. Complaint for Permanent Injunction and Other Relief at 3, FTC v. Kochava, Inc., No.: 2:22-cv-377 (D.C. Idaho Aug. 29, 2022).

134. *Id.* at 6, 10.

135. *FTC Sues Kochava for Selling Data That Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations*, FED. TRADE COMM'N (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

revise its allegations against Kochava.[136] As a result, forward change in legislation on the sale and use of sensitive information has yet to occur.

1. Where Will Our Data Stored in Counterfeit Items End Up?

The data monitoring functions of smart products available to consumers raise the question of how counterfeit items and piracy will be regulated in the business of clothes and accessories. Everyday items like footwear, handbags, electronics, and even medicines have been mimicked and sold to consumers at the expense of a legitimate company.[137] Smart apparel may soon enter the stream of commerce to be equally faked and sold to budget-conscious consumers or unsuspecting consumers who may not know the difference between a genuine and fake item. Consumers would be able to buy fake smart devices at an affordable price, but technological trends beg the questions of where and to whom the consumer's data is going, particularly sensitive personal information like geolocation coordinates of a child wearer.

Companies that produce counterfeit or bargain items made with cheap materials, or that are less known and are simply testing the waters of the law, may be tempted to experiment with what they can get away with. Although developers of mobile apps are required to provide a privacy policy disclosing how a consumer's personal data will be used and accessed, a company may initially choose to provide a generic cookie-cutter policy before any serious investigation into their business practices commences.[138] Could this have been the case with Hilfiger's Awear Solutions' mobile app that was removed from the app stores? Along the lines of unlawful third-party access to personal data, consumers should be concerned about protecting their information from fraudsters in the apparel industry because many items are not subject to the same standards of quality as genuine products.[139] However, fashion brands that produce less expensive smart apparel may still sell unauthenticated products that were produced without the necessary oversight or appropriate materials.

---

136. Tyler Clifford, *Judge Tosses FTC Lawsuit Accusing Broker of Unfair Geolocation Data Sales*, REUTERS (May 5, 2023, 8:22 PM), https://www.reuters.com/legal/judge-tosses-ftc-lawsuit-accusing-broker-unfair-geolocation-data-sales-2023-05-05/.

137. Shane Hickey, *Whether You're Unaware or Don't Care, Counterfeit Goods Pose a Serious Threat*, THE GUARDIAN (Dec. 2, 2018, 3:00 PM), https://www.theguardian.com/technology/2018/dec/02/whether-youre-unaware-or-dont-care-counterfeit-goods-pose-a-serious-threat; *Combating Trafficking in Counterfeit and Pirated Goods*, DEP'T OF HOMELAND SEC. 16-17 (Jan. 24, 2022), https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf [hereinafter *Report to the President*]; Vega Bharadwaj et al., *U.S. Intellectual Property and Counterfeit Goods - Landscape Review of Existing/Emerging Research*, 28-29 (USPTO Econ. Working Paper, Paper No. 2020-03, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3577710#paper-citations-widget [hereinafter *USPTO Report*].

138. *Prepare Your App for Review*, GOOGLE SUPPORT, https://support.google.com/googleplay/android-developer/answer/9859455?hl=en (last visited Sept. 1, 2023).

139. Report to the President, *supra* note 137, at 13, 15, 21; USPTO Report, *supra* note 137, at 15, 28, 36.

B. Actual Knowledge of Child Users and the Apparel Audience Categories

Regarding the requirement that mobile app developers have actual knowledge of collecting children's data, it is unclear whether the apps for smart clothing will fall under a mixed audience or a general audience. Clothes produced for children typically have a limited size range and feature youthful styles, bright colors, or graphics that appeal to children, so it would be more obvious at times if clothes are child-directed. But it will be less obvious for clothing marketed to teenagers where children under thirteen are not the primary audience but are still capable of wearing these types of clothes. Subject to a changing audience, a company's obligations for consent under COPPA may be inconsistent. People come in all different sizes and often wear whatever is available, so maybe a child will make a personal choice to wear clothes intended to be worn by adults. How will this affect age-screening processes or lack thereof on mobile apps for smart apparel? After weighing the child-directed factors mentioned above,[140] the FTC may still find the clothes to be child-directed despite the manufacturer's stated intent. Further, a points-redeeming rewards system like Hilfiger's may fall into the "multiple-contact" exception to parental consent depending on how the child user receives discounts on the mobile app.[141] While smart apparel brands could turn shopping into a fun rewards-earning app-based game for children, such an activity no longer appears to be strictly reserved for children, as evidenced by Hilfiger's app.

Unfortunately, the actual knowledge requirement is vulnerable to loopholes. It may incentivize companies to demonstrate willful disregard by claiming that they do not know to what type of audience they direct their smart apparel mobile app.[142] If a company's app is directed at general audiences, there is no need to investigate the age of each user with an age screen.[143] The company will only be liable under COPPA if they have knowledge of collecting children's data *after the fact*.[144] Brands may claim they believed they were collecting data from adults who had consented to data use, or they intentionally marketed certain products for all ages. It is difficult for companies to truly know the age of their users and the current methods to obtain VPC will likely fail when considering the necessity of wearing clothes.

---

140. *See supra* Section II.

141. *Exceptions to Prior Parental Consent*, Section J(1) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#J.%20Exceptions%20to%20Prior%20Parental%20Consent (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section J(1)*] (explaining that if an operator uses this exception if it expects to contact the child more than once for contests, it must provide parents with direct notice, an opportunity to opt out, and an assurance that it will not use the child's contact information for any other purpose); 16 C.F.R. § 312.4 (c)(3) (2013).

142. Davies, *supra* note 32.

143. *Complying with COPPA Section H(1)*, *supra* note 91.

144. *Id.*

1. Is Data Retained in Regifted or Second-Hand Clothing?

As previously mentioned, COPPA states that companies may retain a child's personal information but "for only as long as is necessary to fulfill the purpose for which [it] was collected."[145] Accordingly, companies must "delete [the] information using reasonable measures to protect against [its] unauthorized access or use."[146] The retention of too much information for a long period of time may lead to security risks and impermissible access to data by hackers.[147] But the FTC has alleged that mobile app developers like Everalbum, Inc. have repeatedly broken the data retention rule.[148] In *In the Matter of Everalbum, Inc.*, the developers of a mobile photo app allegedly retained photos and videos of users who had deactivated their account when users were assured that the media would be deleted upon deactivation.[149] Just like data stored on any mobile app, the data collected from smart apparel will be retained on the user's mobile device at some point before erasure. Unless Bluetooth technology evolves into something that directly tracks the clothes on its own, it is of some comfort that this current technology will not actively track the literal wearer unless they have connected their smartphone to the Bluetooth chip in the clothing. But donating or regifting smart clothes, disconnecting from the Bluetooth smart chip, and deleting the affiliated mobile app cannot guarantee that the previous owner's data tracked by the product is gone forever.

C. Targeted Ads by Alcohol Vendors, Gambling Facilities,… and Balenciaga Campaigns

COPPA compliance of smart apparel brands will depend on whether the brand self-identifies its products as a service geared toward children under the totality of the circumstances.[150] This standard will consider if the products are child-directed or intended for mixed audiences based on the balancing factors mentioned above.[151] Companies want to generate revenue by directing advertisements of child-directed products, like toys, to children, but marketing to children can be harmful. The global fashion industry consistently mistreats children.[152] Considering mistreatment of children in advertising, luxury fashion house Balenciaga recently published an ad campaign that featured children holding

145. 16 C.F.R. § 312.10 (2013).

146. *Id.*

147. David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 OHIO N.U. L. REV. 493, 502 (2016).

148. Complaint at 6, In the Matter of Everalbum, Inc., No. C-4743 (F.T.C. May 7, 2021).

149. *Id.* at 4-6 (explaining that the company also allegedly deceived consumers about its use of facial recognition technology without express user consent).

150. *Complying with COPPA Section H(5)*, *supra* note 83.

151. *Supra* Section II; 16 C.F.R. § 312.2 (2013).

152. *See* UNICEF, CHILDREN'S RIGHTS IN THE GARMENT AND FOOTWEAR SUPPLY CHAIN 4 (June 2020), https://www.unicef.org/reports/childrens-rights-in-garment-and-footwear-supply-chain-2020.

handbags in the shape of teddy bears wearing black leather bondage gear.[153] The brand was accused of "normalizing sexual fetishizations and abuse of children" because some of these images included age-inappropriate items like flasks and wine glasses while another photo's drinking straw was perversely positioned below a child model's legs.[154] Additionally, their subsequent campaign advertising professional women's clothing featured legal documents from *United States v. Williams*, a Supreme Court case that ruled on pandering and possessing child pornography.[155] Balenciaga sued the production company and the set designer for "associat[ing] Balenciaga with the repulsive and deeply disturbing subject of [U.S. v. Williams]," but dropped the lawsuit likely because it only drew attention to the fact that the brand had the final say in the photo approval process.[156] Shortly after Balenciaga's arguably shameful ads, high-end luxury fashion house Gucci photographed singer-songwriter Harry Styles, an adult man, posing next to and carrying a toddler mattress.[157] One of Styles's photos featured a pair of green gingham pants, which he is photographed wearing elsewhere, draped over the mattress.[158] These sister brands, both owned by the same parent company, affirmatively decided to prioritize profits over protection of children and child imagery.

COPPA's child-directed balancing factors as applied to Balenciaga's campaign images strongly suggest its images are directed towards children. The presence of child models and the teddy bears, despite their leather gear, is subject matter that attracts child consumers whereas the dominant black and gray colors do not. Notably, this particular photographer was known for traveling through different countries to take photos of children posed with their favorite items or

153. Jess Cartner-Morley, *Balenciaga Apologises for Ads Featuring Bondage Bears and Child Abuse Papers*, THE GUARDIAN (Nov. 29, 2022, 12:00 PM), https://www.theguardian.com/fashion/2022/nov/29/balenciaga-apologises-for-ads-featuring-bondage-bears-and-child-abuse-papers.

154. *See* Adriana Diaz, *Balenciaga 'BDSM Teddy Bear' Photographer Speaks Out Amid Backlash*, N.Y. POST (Nov. 23, 2022, 2:24 PM), https://nypost.com/2022/11/23/balenciaga-bdsm-teddy-bear-photographer-addresses-backlash/; Erin Keller, *Balenciaga Pulls Controversial Bear Ads Amid Child Abuse Fears*, N.Y. POST (Nov. 22, 2022, 10:18 PM), https://nypost.com/2022/11/22/balenciaga-pulls-controversial-bear-ads-amid-child-abuse-fears/.

155. Elizabeth Paton et al., *When High Fashion and QAnon Collide*, N.Y. TIMES (Nov. 28, 2022), https://www.nytimes.com/2022/11/28/style/balenciaga-campaign-controversy.html; United States v. Williams, 553 U.S. 285, 297-99 (2008) (upholding a federal criminal prohibition against child pornography by excluding offers or requests to obtain such material from protection of the First Amendment).

156. Summons with Notice at 2, Balenciaga v. North Six, Inc., No. Unassigned (Sup. Ct. Nov. 25, 2022); The Fashion Law (@thefashionlaw), INSTAGRAM (Dec. 2, 2022), https://www.instagram.com/p/Clrgv2TOJrb/; Mimosa Spencer, *Balenciaga Designer, CEO Apologize for Ad Campaign Featuring Children*, REUTERS (Dec. 2, 2022, 4:38 PM), https://www.reuters.com/business/retail-consumer/balenciaga-designer-ceo-apologize-ad-campaign-featuring-children-2022-12-02/.

157. Erin Keller, *Gucci and Harry Styles Slammed for 'Sick' Ad With Child's Bed and Teddy Bear Shirt*, N.Y. POST (Dec. 19, 2022, 4:38 PM), https://nypost.com/2022/12/19/gucci-and-harry-styles-slammed-for-sick-ad-with-childs-bed-and-teddy-bear-shirt/.

158. Hayley Peppin & Ella Sangster, *HA HA HA: We Have Our First Look at Harry Styles in His Gucci Collaboration Campaign*, HARPER'S BAZAAR, https://harpersbazaar.com.au/gucci-colloborates-with-harry-styles-for-first-capsule-collection/ (last visited Sept. 1, 2023).

toys.[159] The collection of toys and the chance to show them off is a child-oriented activity that weighs in favor of the content of these images being directed at children. It is disturbing that the brand insinuated items like candles placed inside beer cans were some of the child's most prized possessions. Children using smart devices could have been exposed to these ads if the ads were allowed on child-directed mobile apps because their content appeared directed towards a child audience.[160] Seeing this type of marketing content may encourage impressionable children to make unhealthy choices. Children want to fit in on social media and may be manipulated into desiring products popularized by trendy apparel brands. They are more likely to make irresponsible decisions by seeing certain items, like alcoholic beverages, in advertisements targeted to them. Thus, marketing that is targeted directly at children or featuring COPPA's child-directed factors should not contain anything likely to result in the child's physical, mental, or moral harm. Balenciaga's campaign products were directed to adult consumers but contained content appealing to child consumers. This ambiguity raises the question of how commercial practices and marketing for children's smart apparel will be policed.

IV. TAILORING: CUSTOM REGULATION BECAUSE THE NEXT REVISION IS LONG OVERDUE

Privacy laws typically share standardized consumer rights, such as the right to be informed of certain types of data use and the right to data erasure.[161] However, U.S. privacy laws have not standardized the right for parents to opt out of having their children's data collected for direct marketing purposes. While certain types of marketing can be harmful to children, parents could benefit from companies tracking their children's clothes for purposes of location-finding, particularly where children have gone missing or have been abducted. Therefore, COPPA's geolocation regulations should be amended to distinguish between defined uses for tracking a child's location. Leading up to the FTC's last revision of COPPA in 2013, a commentator for the kidSAFE Seal Program stated "there should be a legal difference between using geolocation information for convenience or to protect a child's safety and to market to a child."[162] The commentator argued that collected location data should "only be considered 'personal information' when it is being used for marketing purposes."[163] However, the FTC responded that it "sees no

159. Sarah LeTrent, *'Toy Stories' Shows Kids with Their Favorite Toys*, CNN (Mar. 17, 2014, 9:53 PM), https://www.cnn.com/2014/03/17/living/toy-stories-photo-book-galimberti/index.html.

160. It is also worth asking how Artificial Intelligence can accurately recognize and distinguish advertisements directed to adults or children based on ad content.

161. Fredric D. Bellamy, *U.S. Data Privacy Laws to Enter New Era in 2023*, REUTERS (Jan. 12, 2023, 10:21 AM), https://www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/; CAL. CIV. CODE §§ 1798.100(b), 1798.105(a) (Deering 2018); VA. CODE ANN. §§ 59.1-577(A)(3), 59.1-578(A)(1) (2023); COLO. REV. STAT. §§ 6-1-1306(1)(a)(IV)(C)(b), (d), 6-1-1308(1)(a)(I)-(V).

162. Children's Online Privacy Protection Rule, 78 FED. REG. 3972, 3982 (2013) (stating kidSAFE Seal Program is defined as an "independent safety certification service and seal-of-approval program designed exclusively for child-friendly websites and technologies.").

163. *Id.*

basis for making the suggested revisions" and that it "prefers to adhere to the statutory language" of the current Rule.[164] With advancements in smart technology, there is now a basis for the FTC to change its mind and distinguish between two smart apparel tracking uses for either marketing or non-marketing purposes.

With a point-redeeming mobile app, a company is in the business of collecting geolocation data for marketing purposes to serve users directed ads based on their behavioral patterns and past purchases.[165] This creates brand loyalty as the consumer uses the app to buy more products and generates ad revenue for the company. A company may also collect personal data for non-marketing purposes, which includes statistical research studies that could improve business operations with knowledge of a user's characteristics or post-purchase behavior.[166] COPPA grants parents the right to prohibit companies from disclosing their child's personal data to third parties generally.[167] However, COPPA in its current form does not grant parents a right to opt in to geolocation tracking and, at the same time, object to a company's processing of their child's geolocation for harmful direct marketing purposes.[168] COPPA mandates that companies give parents specific rights over their children's data, but it does not require companies to offer parents a selective option to opt out of geolocation data collection depending on its eventual use.[169]

The FTC should revisit the commentator's concerns and revise its geolocation regulation to account for smart apparel brands directly tracking the location of clothing for non-marketing purposes. The FTC is advised to review the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) for inspiration as to how to improve COPPA's selective privacy options.[170] Both laws include a focus on data minimization, or the practice of limiting data collection and processing only to the extent that is necessarily required for the service's purposes.[171] This "pseudonymization"

---

164. *Id*. at 3982-83.

165. Jean-Pierre Zreik, *Geo-Location, Location, Location*, 45 RUTGERS COMPUT. & TECH. L. J. 135, 141-43 (2019).

166. Children's Online Privacy Protection Rule, 78 FED. REG. 3972, 3981 (2013) (noting the FTC stated that "statistical reporting" is an activity that is sufficiently covered by the language permitting activities that "maintain or analyze" the functions of the Web site or service within the definition of "support for the internal operations"); 16 C.F.R. § 312 (2013).

167. *Verifiable Parental Consent,* Section I(9) of *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#I.%20Verifiable%20Parental%20Consent (last visited Aug. 31, 2023) [hereinafter *Complying with COPPA Section I(9)*]; 16 C.F.R. § 312.5(a) (2013).

168. *See* 16 C.F.R. § 312 (2013).

169. 16 C.F.R. §§ 312.4(a), 312.5(a)(1), 312.6 (2013).

170. *See generally* Regulation 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 [hereinafter *General Data Protection Regulation*]; Cal. Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100 - 1798.199 (2023).

171. General Data Protection Regulation, O.J. 2016 (L 119) 35; California Consumer Privacy Act, S.B. 1121, 2018 Leg. (Cal. 2018); CAL. CIV. CODE § 1798.140(t)(2)(C)(ii) (Deering 2018);

implements mechanisms during the processing of data that render the information "no longer attributable to a specific consumer without the use of additional information" as long as the mechanisms in place keep the data separated.[172]

The GDPR is a transparent privacy regulation that governs companies targeting or collecting data from EU citizens.[173] Under its conditions for processing the personal data of a child, the GDPR considers consumers under the age of sixteen to be children.[174] Under this law, companies are required to obtain the consent of a parent or guardian in order to collect a child's data, though member states may lower the age to thirteen.[175] Uniquely, the GDPR permits its citizens to object to specific types of data processing.[176] Users of all ages are granted an absolute right to object to a company's processing of their data for direct marketing or research purposes.[177] Thus, it is feasible for U.S. companies to offer the same type of data access selectivity that better protects their consumer's personal information.

California enhances its citizens' privacy rights under the CCPA, but this privacy law is weaker than the GDPR in that it only gives parents a right to object to data collection for sales purposes.[178] California became the first in the U.S. to closely regulate how businesses serving its residents protect, collect, and process their sensitive data.[179] However, this privacy law does not grant consumers an absolute right to opt out of having their data collected for marketing purposes.[180] Still, this law importantly offers parents the choice to opt out of their child's personal data being sold to third parties.[181]

Under COPPA, a parent would first consent to a company's location tracking of the chip embedded in their child's smart clothes. When consenting to precise geolocation data collection, parents should be given the option to selectively opt in for precise location tracking only for non-marketing purposes, like for the parent's interest in locating or tracking their child's movements. Of course, there are GPS mobile apps and products for the very purpose of locating a child, but

---

Bernard Marr, *Why Data Minimization Is an Important Concept in the Age of Big Data*, FORBES (Mar. 16, 2016, 3:24 AM), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/?sh=62c4b1861da4.

172. DATA GUIDANCE & FUTURE OF PRIV. F., COMPARING PRIVACY LAWS: GDPR V. CCPA 16 (2019), https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf.

173. General Data Protection Regulation, *supra* note 170, at 1.

174. *Id.* at 37.

175. *Id.*

176. *Id.* at 45-46.

177. *Id.*

178. CAL. CIV. CODE § 1798.120(c) (Deering 2018).

179. *Understanding the California Consumer Privacy Act (CCPA)*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/understanding-california-consumer-privacy-act (last visited Sept. 1, 2023).

180. *See* DATA GUIDANCE & FUTURE OF PRIV. F., COMPARING PRIVACY LAWS: GDPR V. CCPA 30-31 (2019), https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf (comparing CCPA's right to opt out of the sale of personal data with the GDPR's general right to object to processing other than for direct marketing).

181. CAL. CIV. CODE § 1798.120(b)-(c) (Deering 2018).

these services rely on the child having a handheld device on them at the time.[182] To prevent another *OpenX* or *InMobi* possibility, the FTC can enable this process by revising COPPA's requirements and free consumers from commercial exploitation like targeted geolocation advertising. COPPA could mandate that companies include in their privacy practices a way that allows parents to be more selective about geolocation tracking permission. Without a standardized requirement that companies must offer parents a customized absolute right to object to data collection for direct marketing purposes, companies are incentivized to provide a general all-or-nothing option that is not forward-looking. Instead, having a custom opt in or opt out standard gives the consumer more control over how a company will use their data because the consumer is able to give permission for the specific purposes they desire. Such a standard will give the consumer full control over what geolocation information they choose to share.

Due to the patchwork of federal and state privacy laws in the U.S. that only governs separate types of personal data collection practices, the consumer's right to restrict marketing purposes appears to be statute- and state-specific rather than national. As long as there is no federal U.S. children's privacy law that authorizes the right to opt out of direct marketing purposes, state privacy laws will continue to remain lenient on company data collection practices.[183] The U.S. should follow the EU's example and prioritize human rights over user experience.

As previously mentioned, the GDPR considers the digital age of consent to be sixteen.[184] In the instance of companies selling a child's personal data, the CCPA includes an opt-in requirement for children between the ages of thirteen and sixteen, though parents must still consent on behalf of children under thirteen.[185] Numerous bills have been introduced to change the definition of "minor" or "young consumer" by raising the age of digital consent from thirteen to sixteen, seventeen, or eighteen years old likely because young people are still developing their biological maturity at these ages and young consumers may still be affected by online content.[186] The bills propose various solutions like a blanket ban on advertising that targets teenagers or adding "constructive knowledge" to "actual knowledge" where operators would be liable for unlawful data access if they

182. Tim Lewis, *Honey, Let's Track the Kids: The Rise of Parental Surveillance*, THE GUARDIAN (May 1, 2022, 3:00 PM), https://www.theguardian.com/media/2022/may/01/honey-lets-track-the-kids-phone-apps-now-allow-parents-to-track-their-children (comparing the different types of location tracking apps and watches commonly used by families).

183. Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-577(A)(5) (2023); Colorado Privacy Act, COLO. REV. STAT. § 6-1-1306(1)(a)(I)(A) (2023); Utah Consumer Privacy Act, UTAH CODE ANN. §§ 13-61-201(4)(a) (LexisNexis 2023); Connecticut Data Privacy Act, Substitute S.B. 6, 2023 Leg., Pub. Act 22-15 § 4(a)(5)(A) (Conn. 2023) (comparing state privacy laws providing consumers with the right to opt out of processing personal data for targeted advertising and the sale of personal data).

184. General Data Protection Regulation, *supra* note 170, at 37-38.

185. CAL. CIV. CODE § 1798.120(c) (Deering 2018).

186. H.R. 5703, 116th Cong. § 2 (2020), https://www.congress.gov/bill/116th-congress/house-bill/5703; S. 1628, 117th Cong. § 3(a)(18) (2022), https://www.congress.gov/bill/117th-congress/senate-bill/1628; S. 748, 116th Cong. § 3(a)(19) (2019), https://www.congress.gov/bill/116th-congress/senate-bill/748/text.

should have reasonably known they collected data from child users.[187] The Supreme Court has held that an age restriction on children buying video games without parental consent is unconstitutional under the First Amendment for restricting speech.[188] Opponents of COPPA lament that parents who keep their children from participating in social media are depriving them of educational or social opportunities.[189] Age restrictions only delay the inevitable outcome that children are taught to lie about their age to bypass age gates. Research suggests that consumers younger than even eleven are aware of the risks and consequences of sharing private information, but young people obtain such wisdom and discernment at different ages.[190] Children's First Amendment rights should still be supported without a sacrifice of personal data protection. This is why online services and mobile apps for smart apparel must offer consumers an easy-to-use interface with customizable personal data access options. Rather than agreeing to adhesion-like, conditional privacy policies that would prevent a user from using their service if not agreed to, customizable policies would not prevent users from being able to use the service.

The next COPPA revision should give parents the ability to selectively consent to a company's enumerated privacy practices affecting their child's data. Having a straightforward mobile app interface will likely benefit users by giving them informed consent to make personal data access decisions. Consumers should have full customization ability on how their personal information may be used by smart apparel brands. Especially true at the beginning of social networking and digital advertising, there may still be a general lack of understanding of how personal data is harvested from these sites. The Children and Teens' Online Privacy Protection Act bill (CTOPPA) proposes that mobile apps directed at children must meet appropriate data security standards and prominently display an easy-to-understand privacy dashboard detailing how information is collected, transmitted, retained, used, and protected.[191] A page that outlines what the company does with the user's data should naturally lead to a page where the user may consent to or deny the individual aspects with clear descriptions on how to opt in or out. Easy-to-follow directions within an opt out system should be offered to consumers using smart apparel apps, like a point-redeeming app based on personal data. Companies should not assume consent and consumers should be provided with the ability to opt out of certain data collecting components within their smart devices while still being able to use the product for its functional

187. H.R. 5703, 116th Cong. §§ 3(2)(a), (6)(A)(ii) (2020); S. 1628, 117th Cong. §§ 3(1), 6(a)(1) (2020); S. 748, 116th Cong. §§ 3(1), 6(a)(1) (2019).

188. Brown v. Ent. Merch. Ass'n, 564 U.S. 786, 804-05 (2011) (holding violent video games qualify for First Amendment protection as protected speech and can be sold without parental supervision because the games communicate ideas and possibly social messages).

189. Erin Spain, *Why Parents Help Their Children Lie to Facebook About Age*, NORTHWESTERN (Nov. 1, 2011), https://www.northwestern.edu/newscenter/stories/2011/10/hargittai-facebook-underage.html.

190. Jun Zhao et al., *'I Make Up a Silly Name': Understanding Children's Perception of Privacy Risks Online* 106 (Proc. of the 2019 CHI Conf. on Hum. Factors in Computing Sys. May 2019), https://dl.acm.org/doi/10.1145/3290605.3300336.

191. S. 1628 117th Cong. § 8(a) (2021-2022).

purpose. At this time, luxury fashion brands have few procedures to follow to set a precedent. The legal field in this era of new smart clothing demands more transparent guidelines and higher standards of consumer data privacy.

CONCLUSION: A FINISHED PRODUCT

This Note asks that the FTC amend COPPA and clarify the scope of this important children's privacy law in relation to children's smart clothes. Smart apparel calls into question how consumer privacy will be protected regarding counterfeit items and the ability of brands to unlawfully retain data collected from mobile apps that track the consumer. These concerns are further fueled by the ambiguity in COPPA's actual knowledge requirement and the distinct audience categories to which companies direct their service. Further, precise geolocation tracking has been shown to exploit child consumers, and mobile users are entitled to selectively consent to data collection for non-marketing purposes based on this evidence. Under the right to privacy, it is important that all consumers have selective control over how brands access certain types of the consumer's personal data. Therefore, privacy policies and company data collection practices should be revisited to give consumers proper informed consent to data usage. In its current form, COPPA's ambiguous language will likely result in fashion brands' unlawful access of children's personal data based on the information their smart apparel collects. Let us begin COPPA's next amendment with the thought of children's welfare as a paramount concern.