

common sense®

2023

State of Kids' Privacy

Who is monetizing our data? A general lack of transparency leads to a confusing landscape.

Credits

Authors: Girard Kelly, Common Sense Media
Jeff Graham, Common Sense Media
Steve Garton, Common Sense Media

Contributors: Jill Bronfman

Data analysis: Girard Kelly, Common Sense Media
Jeff Graham, Common Sense Media

Copy editors: Christopher Dare, Common Sense Media
Tasha Kelter

Designer: Jeff Graham, Common Sense Media

Photo: © iStock/StefaNikolic

Suggested citation: Kelly, G., Graham, J., & Garton, S. (2023). *2023 State of Kids' Privacy: Who is monetizing our data? A general lack of transparency leads to a confusing landscape.* San Francisco, CA: Common Sense Media

This work is licensed under a Creative Commons Attribution 4.0 International Public License.

Table of Contents

Abstract 1

Introduction 1

The Increased Awareness of Selling Data 2

The California Consumer Privacy Act (CCPA) 3

Defining Selling or Sharing Data 4

Confusing Sharing But Not Selling Data 5

Evaluating Selling or Sharing Data 6

Selling Data and Cross-Context Behavioral Advertising 7

Sell Data Evaluation Question 7

Third-Party Tracking Evaluation Question 8

Track Users Evaluation Question 9

Ad Profile Evaluation Question 9

Selling Data Multiple Privacy Practice Comparison 10

Data Sold: "Better" 10

Data Sold: "Worse" 12

Data Sold: "Unclear" 13

Examples of Selling Data Disclosures 13

Transparently Better 13

Transparently Worse 14

Disagreement 14

Confusion 14

Inconsistencies 14

Obfuscation 16

Unclear 16

California Only 17

Limited Protections 17

Companies Need to Disclose That They Sell Your Data 18

Conclusion 20

Abstract

This paper is the Common Sense Privacy Program's 2023 in-depth analysis regarding the practice of selling data for 200 of the most popular products used by kids and families. Our data indicates that the majority of companies whose privacy policies say they do not sell or share users' data to third parties actually have other forms of data monetization practices that would likely be *considered* selling or sharing data under new California Privacy Rights Act amendments. In addition, companies with policies that remain non-transparent on the practice of selling or sharing data and that are also non-transparent on the use of other data monetization practices—such as the use of third-party tracking, tracking users across the internet, or the creation of advertising profiles for commercial purposes—are presumed likely to be selling data, as supported by our long-term research.

The passage of the California Privacy Rights Act (CPRA), which amended the California Consumer Privacy Act (CCPA), expanded the definition of selling data to include whether a consumer's data is "sold or shared" with third parties for "cross-contextual advertising." The Common Sense Privacy Program reads and evaluates the privacy policies of hundreds of the most popular applications and services used by children, students, parents, educators, and consumers. In this paper, we use these privacy evaluations and respective data to analyze multiple privacy practices that are now covered under the CPRA, and illustrate how companies are inaccurately informing consumers about various forms of data monetization used to sell consumers' data to third parties.

Our results indicate that in 2023, 73% of the industry should be disclosing in their privacy policies that they are selling consumers' data, and 48% of the industry is likely not in compliance with the CCPA's requirement that businesses disclose whether a consumer's personal information is "sold or shared" to third parties.

Introduction

The Common Sense Privacy Program[1] has created a standardized framework to describe and analyze information in privacy policies so that parents and caregivers, teachers, and consumers can make smart and informed choices about the tools they use for themselves and with their children and students. And with the involvement of over 400 schools and districts,[2] Common Sense is working in collaboration with third-party software developers of some of the products we evaluated to bring greater transparency to privacy policies across the industry. We have been collecting and incorporating feedback from various stakeholders about how to share the results of our privacy evaluations since our first State of EdTech report was published in 2018.[3] We have spoken with numerous children, teens, students, educators, parents, developers, consumers, companies, privacy advocates, policymakers, and industry representatives about their perspectives on privacy to help inform our work.

Our previously released 2021 State of Kids' Privacy report[4] represented the culmination of our research over the previous four years in evaluating hundreds of applications and services geared toward kids, consumers, and the education sector. This paper focuses primarily on changes to consumer privacy laws and the practice of selling data. When speaking to parents, educators, and consumers, we consistently hear that "selling data" is one of the most important, if not the most important, privacy issues that they want to quickly and confidently understand before using a product.[5] Consumers often say they feel incapable of providing meaningful consent when it comes to how companies use their data, and our research illustrates that most companies do not give consumers a meaningful choice to provide consent because they fail to provide adequate notice to consumers of their actual privacy practices.

This paper has been directly impacted by consumer privacy laws that were passed in 2018, including Europe's General Data Protection Regulation (GDPR),[6] which provides individual data rights and allows data subjects to withdraw consent or object to the sale of their personal information. In addition, U.S. state legislation—such as the California Consumer Privacy Act (CCPA) in 2019 and the subsequent California Privacy Rights Act (CPRA)[7] amendments to the CCPA in 2020—now provides consumers with the right to opt out of the sale of their personal information to third parties. Privacy policy changes that began in 2018 accelerated in the following years due to the passage of the CCPA, the CPRA, and a patchwork of other U.S. state-specific consumer privacy laws that were introduced in state legislatures around the country due to a lack of a comprehensive federal consumer privacy protection law.[8] As a result, the

[1] Common Sense Media, Privacy Program, https://privacy.commonsense.org.

[2] Common Sense Media, District Privacy Consortium, https://privacy.commonsense.org/resource/district-consortium.

[3] Kelly, G., Graham, J., & Fitzgerald, B. *2018 State of Edtech Privacy Report*, Common Sense Privacy Evaluation Initiative. San Francisco, CA: Common Sense (2018), https://www.commonsense.org/education/articles/2018-state-of-edtech-privacy-report.

[4] Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2021). *2021 State of Kids' Privacy*. San Francisco, CA: Common Sense Media, https://www.commonsensemedia.org/research/state-of-kids-privacy-report-2021.

[5] Americans Can't Consent to Companies' Use of Their Data, Annenberg School for Communication (Feb. 10, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4391134.

[6] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

[7] California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.100-1798.198.

[8] International Association of Privacy Professionals (IAPP), US State Privacy Legislation Tracker, https://iapp.org/resources/article/us-state-privacy-legislation-tracker.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

privacy policies we examined changed in waves, and the privacy practices were enabled on the exact dates when each of these new laws and regulations took effect. In many cases, policy edits closely followed the letter of the new laws, and the increased transparency resulted in the disclosure of privacy-invasive or privacy-compromising practices, which we have summarized as "worse" practices.

While we closely examine new statutes and regulations and assign points for transparency in the policies, we also seek to identify and promote privacy-preserving practices that go beyond the letter of these laws, which we have summarized as "best" practices. As a consequence, we are keenly attuned to small differences in the wording of privacy policy provisions that specifically limit the promises of new rights and abilities to a particular jurisdiction or type of user, versus those that expand the application of the new laws to all users. In some cases it may be appropriate to limit privacy protections to children under the age of 13, such as for parental permissions. However, it is almost never ethically defensible to limit a privacy protective provision to just someone in the state of California while denying such protection to someone in a neighboring state. Many companies may look at their own logistics and operational costs and discover it is easier and less expensive for their company to offer privacy protections to all users, due to economies of scale and the transactional costs of compliance. Our evaluation process awards the most points for transparency and "better" practices to policies that grant privacy protections to all users, regardless of the jurisdictional legal obligation.

The Common Sense Privacy Program was created to champion child and student privacy and support parents, educators, schools, and policymakers on a path toward a more secure and safe future for all kids.

In order to effectively evaluate the policies of all these applications and services, we developed a comprehensive, standardized framework based on existing international, U.S. federal, and U.S. state law, as well as privacy and security principles and industry best practices.[9] This framework incorporates over 150 privacy- and security-related questions that are expected to be answered in policies for products used with children or in educational or consumer contexts. In addition, qualitative and quantitative methods were developed to determine both the particular issues that companies disclose in their policies and the meaning behind those disclosures. As a result, the Common Sense Privacy Program has produced a substantial body of work, including these crucial privacy evaluations available to the public for review, analysis, and consumer education for free.[10] The paper covers only a small portion of the conclusions that could be drawn from the rich data created by these evaluations.[11] Looking at the privacy policies and terms of service for the top 200 educational and consumer apps used by children and students is a great way to start illuminating the dark corners of the industry and increasing the standards for kids' privacy.

The Increased Awareness of Selling Data

Selling data to third parties has always been a topic of concern with parents, educators, and consumers because it means users' interactions and behaviors with technology are exploited for profit. Consumers are generally aware that children and student's' personal information has historically been protected from sale to third parties[12], and when surveyed, consumers say they want the same strong privacy protections extended to everyone.[13] Our evaluation question related to selling data was created to capture whether a company's policies disclose if any user's personal information is sold or rented to third parties for monetary or other valuable consideration.[14] Selling users' data is an important issue for a policy to disclose because users want to know if their data is shared with third parties in exchange for use of the product, which may impact their decision whether to use the product or service.

In 2018, the practice of selling data became a bipartisan focal point for the first time in California politics with

[9] Common Sense Media, Full evaluation questions, https://github.com/commonsense-org/privacy-questions-output/blob/main/full-questions.md.

[10] Common Sense Media, Privacy Program, https://privacy.commonsense.org/evaluations.

[11] *See* Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2021). *2021 State of Kids' Privacy*. San Francisco, CA: Common Sense Media, https://www.commonsensemedia.org/research/state-of-kids-privacy-report-2021.

[12] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2; *See also* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(3).

[13] *See* Perrin, A. (2020, April 14), *Half of Americans have decided not to use a product or service because of privacy concerns*, Pew Research Center, https://www.pewresearch.org/facttank/2020/04/14/half-of-americans-have-decided-not-to-use-aproduct-or-service-because-of-privacy-concerns; *See also* Auxier, A., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15), *Americans and privacy: Concerned, confused, and feeling lack of control over their personal information*, Pew Research Center, https://www.pewresearch.org/internet/2019/11/15/americans-andprivacy-concerned-confused-and-feeling-lack-of-control-overtheir-personal-information.

[14] Common Sense Media, Full evaluation questions, Sell Data evaluation question, https://github.com/commonsense-org/privacy-questions-output/blob/main/full-questions.md ("Do the policies clearly indicate whether or not a user's personal information is sold, or exchanged for anything of value to third parties?")

the introduction of ballot proposition 24, the California Consumer Privacy Act (CCPA).[15] This pro-consumer privacy proposition was the result of increased national media attention focused on privacy because of numerous data breaches including Equifax[16], which affected hundreds of millions of consumers, and numerous high-level privacy scandals with whistleblowers revealing third-party data misuse and first-party negligence involving Facebook and Cambridge Analytica.[17] Moreover, it is concerning that the sharing of Facebook users' data with third-party companies for their own research purposes—which is a practice tracked by our *Third-Party Research* evaluation question—was not consistent with the principles of providing notice to users, obtaining informed consent, or allowing participants the ability to opt out.[18]

In order to make an informed decision about the use of a product, existing or potential users need to know if data collected from their use of the product is sold to third parties.

Companies updated their privacy policies in 2018 to overwhelmingly disclose the "better" practice that they did not sell users' data to third parties. This was the result of selling data becoming one of the most controversial and widely known privacy practices among general consumers, with mainstream media headlines and congressional committee hearings discussing Facebook's data misuse scandal involving Cambridge Analytica. Also, companies updated their policies to reflect the recent passage of Europe's General Data Protection Regulation (GDPR), which prohibited the sale of personal information of European users without consent as a legal basis for processing, and privacy laws already protecting the data of children and students from sale, but not consumers. Additionally, state legislation such as the California Consumer Privacy Act (CCPA)[19] pushed for the right for all consumers to opt out of the sale of their personal information to third parties for profit. As a political compromise, the CCPA ballot initiative was retracted. It was later introduced as legislation and passed by the California State Legislature in 2019,[20] and became California state law effective in 2020. However, based on concerns that the nation's first privacy law did not go far enough to protect consumers, the CCPA was quickly amended to strengthen the law with a second ballot initiative called the California Privacy Rights Act (CPRA), which passed and went into effect January 1, 2023.[21] Among numerous additions, the CPRA's amendments broadened the scope of the CCPA's definition of "sale" to include a consumer's right to know if their personal information was "sold or shared" with third parties for *cross-context behavioral advertising*, which is a new legal term meant to include the practice of tracking or profiling users for targeted advertising. The "creepy factor" concept of companies selling a user's data to third parties by tracking their activity without their knowledge or consent for targeted advertising was a primary concern of voters in the passage of both laws, and is the research focus of this paper.[22]

The California Consumer Privacy Act (CCPA)

The CCPA included the following five core rights for consumers:

1. **The right to know** what personal information is collected, used, shared, or sold.
2. **The right to opt out of the sale** of personal information. Children under the age of 16 must provide opt-in consent, with a parent or guardian providing consent for children under 13. Parents can also opt out on behalf of their children.
3. **The right to access, delete, and download** personal information.
4. **The right to non-discrimination** in terms of price or service when a consumer exercises a privacy right under the CCPA.
5. **A private right of legal action** for a data breach where reasonable security protections were not used by the company.

[15] *See* Californians for Consumer Privacy, https://www.caprivacy.org; *See also* Epic, California's Proposition 24, https://epic.org/californias-proposition-24.

[16] *See* Federal Trade Commission (FTC), Equifax Data Breach Settlement: What You Should Know, https://consumer.ftc.gov/consumer-alerts/2019/07/equifax-data-breach-settlement-what-you-should-know.

[17] Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, Mar. 15, 2017, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[18] *See* Adam D. I. Kramer, Jamie E. Guillory, Jeffrey T. Hancock, Experimental evidence of massive-scale emotional contagion through social networks, (Jun. 02, 2014), https://www.pnas.org/doi/pdf/10.1073/pnas.1320040111.

[19] California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100-1798.198.

[20] The CCPA was introduced as AB-375, by Ed Chau, member of the California State Assembly, and State Senator Robert Hertzberg.

[21] *See* the California Privacy Rights Act of 2020, Proposition 24 in the general election of November 3, 2020, https://thecpra.org.

[22] Goodwin Simon, *Summary of Key Findings from California Privacy Survey*, https://www.caprivacy.org/icymi-summary-of-key-findings-from-california-privacy-survey.

The California Privacy Rights Act (CPRA) amendments to the CCPA incorporated many additional rights, including the following 10 most important rights for consumers:

1. Created the right to limit the use of sensitive personal information.
2. Created the right to correct personal information.
3. Extended the right to opt out of sale to include opting out of the "sharing" of personal data.
4. Provided stronger safeguards for kids.
5. Created the right to opt out of automated decision making and profiling.
6. Established the California Privacy Protection Agency (CPPA).
7. Required businesses to provide data protection by default and to perform data protection impact assessments.
8. Expanded the data breach private right of legal action.
9. Increased fines and enforcement ($2,500–$7,500).
10. Reduced the ability to weaken the privacy law in California.

Defining Selling or Sharing Data

The California Privacy Protection Agency (CPPA)[23] finalized regulations implementing the CPRA amendments to the CCPA in March 2023.[24] Companies are required to provide a clear and conspicuous link on the business's internet homepage, titled "Do Not Sell or Share My Personal Information," if they meet the statutory requirements of a covered "Business" and engage in the practice of selling or sharing a consumer's personal information, or they can use the Alternative Opt-out Link such as "Your Privacy Choices" or "Your California Privacy Choices," in accordance with the CCPA.[25,26]

The CPRA amendments define "**sell**," "selling," "sale," or "sold" as selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.[27] In addition, the CPRA introduces the new practice and definition of "**share**," "shared," or "sharing," which means "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for *cross-context behavioral advertising*, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged."[28]

Under the CPRA, the new definition of "**cross-context behavioral advertising**" is "the targeting of advertising to a consumer based on the consumer's *personal information* obtained from the consumer's activity across businesses, distinctly branded websites, applications, or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts."[29] Therefore, any targeted advertising, tracking, or profiling of a consumer with their personal information would constitute selling or sharing their personal information under the CCPA.

"**Personal information**" under the CPRA is included in the definition of "sale," "share," and "crosscontext behavioral advertising" and includes "[i]nferences drawn from any personal information to create a *profile* about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[30] The term "**profiling**' means any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."[31] Profiling for personalized advertising purposes under the CPRA is not considered a legitimate "Business Purpose"[32] and therefore, personal information of a consumer cannot be used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.[33]

[23] California Privacy Protection Agency (CPPA), https://cppa.ca.gov.

[24] California Privacy Protection Agency (CPPA), California Consumer Privacy Act Regulations, https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf.

[25] California Privacy Rights Act (CPRA), Cal. Civ. Code §1798.140(d).

[26] California Consumer Privacy Act Regulations, § 7015. Alternative Opt-out Link, https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf.

[27] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ad)(1).

[28] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ah)(1).

[29] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(k).

[30] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(v)(1)(K).

[31] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(z), (aj).

[32] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e)(4).

[33] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(e)(4).

The intersection of the CPRA's definition of "sell," "share," "cross-context behavioral advertising," "profiling," and "personal information" has created confusion with consumers about whether a company is actually selling their data, sharing their data, or both. Consumers do not understand the legal distinction between the definition of selling or sharing data, and simply want to know if the company or product is making money from their data.

The most important question consumers want to know about a product is whether the company is making money from their data.

Confusing Sharing But Not Selling Data

The CPRA amendments' inclusion of the new right to opt out of the "sale or sharing" of personal information [34] is described as a single consumer right, but with two different "either/or" practices that companies may engage in, which allows for consumers to opt out of one practice, but not the other. Generally speaking, the practice of "selling" data requires: 1) a consumer's personal information, 2) given to a third party, 3) for money or other form of value. The practice of selling data is intended to be a broad definition that is meant to be flexible and adapt to all the possible methods by which a company could potentially monetize a consumer's data. The broad scope of the definition of selling data is meant to include the more specific method and practice of "sharing" data, which requires: 1) a consumer's personal information, 2) given to a third party, 3) for cross-context behavioral advertising, which means targeted advertising, 4) whether or not for money or other form of value. The use of "sale *or* share" language has been perceived by companies as creating several different scenarios that involve both the sale of data and the sharing of data.

Table 1 indicates the nine different ways a company may choose to disclose this information or not; *yes* indicates that the policy discloses the company does engage in the respective practice, *no* indicates the company does not engage in the respective practice, and *unclear* indicates the company makes no meaningful disclosure regarding the respective practice. For example, the second row in table 1 indicates the scenario where a company discloses "no" they do not sell data, and "yes" they may share data under the CCPA. In this scenario, they may only offer a cookie consent preference setting to opt out of targeted advertising. However, in another example indicated by row 6 in table 1, a company's policy may disclose "yes" they sell data, but remain non-transparent or "unclear" on whether they share data, and therefore they may only offer a preference setting to opt out of the sale of data. In situations like row 5 of table 1, where a company's policy says both "yes" they may sell data, and "yes" they may share data under the CCPA, consumers may think they opted out of the sale of their data, when in fact they only may have only opted out of sharing their data through a prominently displayed cookie consent notice. The company may offer a separate mechanism to opt out of sale.

Automated opt-out mechanisms such as the Global Privacy Control (GPC), [35] which is a technical specification for transmitting universal opt-out signals, may be helpful in allowing consumers to automatically send their "opt out of sale" preference under the CCPA. [36] However, these types of opt-out privacy tools have limitations: They must be activated in the consumer's browser on every device; they must be adopted by the company with which the consumer is interacting; and, problematically, these preferences are typically stored in persistent tracking cookies or attached to their user account. Therefore, if consumers clear their cookies or if they are not logged into their account, then automatically sending universal opt-out signals to companies would not protect consumers' anonymous interactions with the company from being sold or shared with third parties for commercial purposes. This is why alternative privacy proposals that would require opt-in consent would better protect all users' privacy: By default, a company would not be able to sell or share a consumer's data without their explicit consent. Universal opt-in consent would also protect users' ability—especially children—to anonymously interact with a company and not have their data inadvertently monetized. Common Sense's evaluation of privacy policies has found that companies disclose the following types of "sale or share" scenarios:

Table 1: Sell data and share data policy disclosure detail.

Sell Data	Share Data
no	no
no	yes
no	unclear
yes	no
yes	yes
yes	unclear
unclear	no
unclear	yes
unclear	unclear

The legislative intent of the definition of selling data was meant to be inclusive of sharing data under the CCPA for commercial purposes because selling data's third factor, "for money or other form of value," is sufficiently broad to cover any sharing of data for the benefit of a business

[34] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.120.

[35] See Global Privacy Control (GPC), https://globalprivacycontrol.org.

[36] *See* California Privacy Protection Agency, Final Regulations, § 7025.

CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL PUBLIC LICENSE

even when no money is exchanged. Consumers have several choices when it comes to exercising their right to opt out of sale or sharing. For example, consumers who opt out of a product selling their data also opt out of sharing for commercial purposes—but consumers can also specifically opt out only of sharing their data, which companies have interpreted as opting out of only targeted advertising, without also opting out of additional forms of data monetization such as selling data to third parties.

Table 2: Consumer opt-out request and subsequent vendor action(s).

Opt-out request	Product sells	Product shares
Sell data	yes, opt-out	yes, opt-out
Share data	no change	yes, opt-out
No request	no change	no change

These different situations can create confusion for companies because they think they do not sell data under the CCPA, but rather only share data with third parties for targeted advertising, which requires the practices of tracking and profiling users. This distinction between sell and share can also confuse consumers who do not assume "sharing" their data with third parties is the primary method that companies use to monetize their data, because the term "sharing data" pre-dates the CCPA or CPRA's appropriation of "share." The phrase "sharing data" is generally understood by consumers as a requirement to make Internet-enabled applications and services "just work." It is not surprising that a majority of companies disclose in their policies that they do not sell data, but just share data for cross-context behavioral advertising, which is a practice they likely already disclosed in their policies as targeted advertising before the CCPA or CPRA amendments came into effect.

The practice of sharing data for cross-context behavioral advertising is considered a form of data monetization.

Alternatively, the CPRA amendments could have included the practice of "disclosing a consumer's personal information for cross-context behavioral advertising to third parties" in the definition of "sell," but cross-context behavioral advertising was included in a new definition of "share" to capture this specific practice and allow separate opt-out requests. We believe this is causing confusion for both companies and consumers. The practice of either selling or sharing data for cross-context behavioral advertising still monetizes users' data, but only sharing data for monetary value is a more specific form of selling. Therefore, for the purposes of our research and this paper, when companies disclose they do not sell data, but rather only share data for cross-context behavioral advertising, it is interpreted to meet the definition of "sell" under the CCPA and the company needs to change its policies to correctly disclose that they sell data.

Evaluating Selling or Sharing Data

The Common Sense Privacy Program created a comprehensive evaluation process for evaluators to answer questions by reading privacy policies for popular mobile applications and online services.[37] Our evaluation process attempts to address some of the common barriers to understanding a product's privacy practices and summarize answers to privacy questions to help users provide meaningfully informed consent, or to choose not to use products as a result of their privacy practices. For example, the following evaluation question requires a reviewer to read the policies of the application or service and determine whether or not they disclose the issue raised in the question by providing a yes or no response:

Question: Do the policies clearly indicate whether or not the company collects personally identifiable information (PII)?

If the reviewer responds yes to this question in our policy annotator software, that means the application or service discloses whether or not it collects personally identifiable information. Given a "yes" transparent response to this question, the evaluator is then asked a follow-up question—a slightly adjusted version of the original attempting to capture if they engage in a particular practice. In this case:

Do the policies indicate the company collects personally identifiable information (PII)?

A yes or no response about whether personally identifiable information is or is not collected will determine the final question points based on whether the practices described are considered qualitatively "better" or "worse" for the purposes of our evaluation process. For the purposes of this paper, our analysis focuses on the intersection of the definition of "cross-context behavioral advertising" and selling or sharing data under the CPRA amendments with the following four evaluation questions:

[37] *See* Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2021). 2021 State of Kids' Privacy. San Francisco, CA: Common Sense Media, pp. 14-15, https://www.commonsensemedia.org/research/state-of-kids-privacy-report-2021.

- **Sell Data**: *Do the policies clearly indicate whether or not a user's personal information is sold, or exchanged for anything of value to third parties?*
- **Third-Party Tracking**: *Do the policies clearly indicate whether or not third-party advertising services or tracking technologies collect any information from a user of the application or service?*
- **Track Users**: *Do the policies clearly indicate whether or not a user's personal information is used to track and target advertisements on other third-party websites or services?*
- **Ad Profile**: *Do the policies clearly indicate whether or not the company allows third parties to use a user's data to create a profile, engage in data enhancement or social advertising, or target advertising?*

However, first-party monetization, which includes our *Personalized Ads*[38] privacy evaluation question, is not included in this data-sold analysis or covered in the *Multiple Privacy Practice Comparison* section below. This is because the CPRA excludes the practice of behavioral or targeted ads—which is often referred to as Personalized Ads—in its definition of cross-context behavioral advertising, when personal information is used for personalized advertising *only* from the *first-party* business, distinctly branded website, application, or service with which the consumer intentionally and directly interacts.[39] Our evaluation question interprets targeted or behavioral ads that are displayed to the user on the first-party platform to be associated with the *Personalized Ads* evaluation question. However, if personal information is shared with *third parties* to display targeted or behavioral ads to users on other third-party applications or services across the internet which the consumer does not intentionally interact with, we categorize that practice with our *Track Users* evaluation question.

[38] Common Sense Media, Full evaluation questions, Personalized Advertising evaluation question, https://github.com/commonsense-org/privacy-questions-output/blob/main/full-questions.md ("Do the policies clearly indicate whether or not advertising based on a user's personal information are displayed on the first-party product?")

[39] See example of first-party advertising. Discord, Privacy Policy, https://discord.com/privacy ("We are proud of the product we've built. We may tell you about our paid services and other features directly in the services and through our own channels, and we spend money advertising Discord on other platforms.") (Accessed April 1, 2023).

Selling Data and Cross-Context Behavioral Advertising

The new CPRA intersection of *cross-context behavioral advertising* is fully represented in our existing *Sell Data*, *Third-Party Tracking*, *Track Users*, and *Ad Profile* evaluation questions, which are expected to include all of a company's data monetization and selling practices. Since our evaluation process has always included these four questions, we can compare their historical practices since 2018—as shown in figure 1 below—and speculate about what "selling" data practices a company should disclose since the CPRA amendments became law in January 2023. As indicated in our *Sell Data* evaluation question, as companies move from non-transparency about selling data to discussing statutory requirements related to selling data such as the CPRA's cross-context behavioral advertising, tracking, and profiling, they will most likely disclose "worse" practices for kids and families. Our results indicate compliance with the CPRA amendments is low, but we expect that companies' transparency will increase in the future. Companies will likely disclose "worse" practices, as covered by the definition of "sale" under the CCPA with our *Sell Data* evaluation question, which is expanded to include "sharing" a user's personal information with third parties for "cross-context behavioral advertising." This change implicates the following four privacy evaluation questions.

Sell Data Evaluation Question

The Sell Data evaluation question indicates whether the policies disclose that a user's personal information is sold or rented to third parties for monetary or other valuable consideration. Selling users' data is an important issue to disclose in the policy because users want to know if their data is shared with third parties in exchange for use of the product and the answer may impact whether they decide to use the product or service.[40,41,42,43,44,45] A "better" response to this

[40] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

[41] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(3).

[42] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.120(b)-(c).

[43] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.135(a).

[44] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ad)(1).

[45] *See* General Data Protection Regulation (GDPR), Art. 13(2)(b), 14(2)(c), 15(1)(e), 18(1)(d), 21(1), 21(4).

evaluation question indicates the product *does not* sell a user's data to third parties. A "worse" response indicates the product *does* sell a user's data to third parties. "Unclear" indicates that no relevant disclosure is made available in the policies.

Figure 1: Sell Data: Do the policies clearly indicate whether or not a user's personal information is sold, or exchanged for anything of value to third parties?

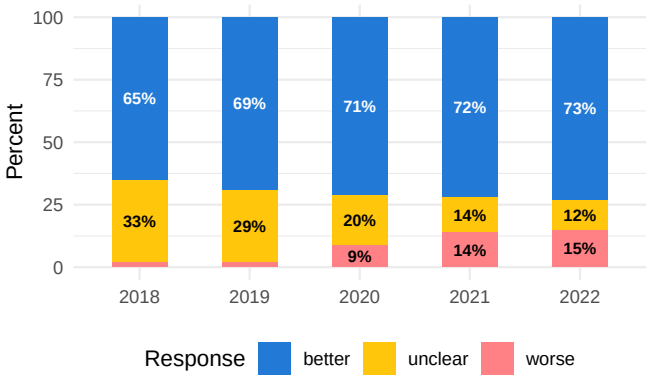


Figure 1 does not indicate any significant differences from 2021 to 2022 in the practice of selling data. We see 73% of companies disclosing the better practice that they do not sell users' data. Additionally, we see a small decrease—from 14% to 12%—in companies not disclosing whether or not they sell data. However, this decrease in non-transparency or "unclear" results in a similar increase from 14% to 15% of companies updating their privacy policies to disclose under the CCPA that they sell users' data. The data from 2022 indicates, similar to prior years, that the vast majority of companies that remain non-transparent about selling data are more likely to already be engaging in the sale of data, but without giving users adequate notice. These companies may continue to remain non-transparent on the practice of selling data for as long as possible in order to minimize their business risk if they disclose the wrong practice and to avoid costly legal consulting fees. Current business practices incentivize remaining non-transparent without an increased risk of regulatory enforcement or customer awareness of their non-transparency. If a company discloses they now sell consumers' data, the change could negatively impact their sales revenue, could decrease marketing leads, and would require expensive legal fees to change their privacy policy and complete a privacy impact assessment of their product to come into compliance.

Third-Party Tracking Evaluation Question

The Third-Party Tracking evaluation question indicates whether the company allows third-party companies to use cookies or other tracking technologies on its product, enabling those third-party companies to collect and use a user's personal information for their own purposes. A company should not permit third-party advertising services or tracking technologies to collect any information from a user who is using the service. A user's personal information provided to a product should not also be used by a third party to persistently track that user's behavioral actions on the product to influence what content they see in the product and elsewhere online. Third-party tracking can influence a user's decision-making without their knowledge, which may cause unintended harm.[46,47,48] A "better" response to this evaluation question indicates that the company *does not* allow third-party companies to use cookies or other tracking technologies on its product. A "worse" response indicates that the company *does* allow third-party companies to use cookies or other tracking technologies on its product. "Unclear" indicates that no relevant disclosure is made available in the policies.

Figure 2: Third-Party Tracking: Do the policies clearly indicate whether or not third-party tracking technologies collect any information from a user of the product for the third party's own purposes including advertising?

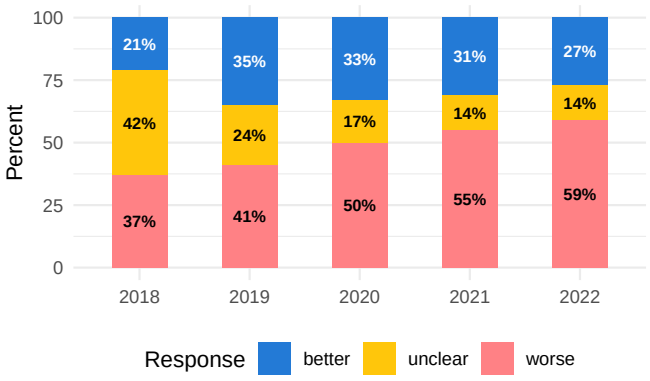


Figure 2 indicates an increase in third-party tracking "worse" disclosures since 2021. We see a small decrease of from 31% to 27% of companies disclosing the better practice that they do not use personal information for third-party tracking purposes. However, there remains no change in the 14% of companies that still do not disclose whether they engage in the practice of third-party tracking. The decrease in better practices unfortunately results in a similar increase from 55% to 59% of companies updating their privacy policies to now disclose under the CPRA amendments that they engage in third-party tracking practices. The increase since 2018 in a company's transparency to disclose "worse" third-party tracking practices in their policies was likely motivated in part because of the passage of Europe's General Data Protection Regulation (GDPR)[49] in 2018. The GDPR included the concept of "tracking" as part of a company's

[46] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

[47] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(7).

[48] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(k), (l), (ah), (aj).

[49] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

legitimate interests to process data for marketing purposes, which may have incentivized companies to describe this data monetization method in their privacy policies so they could obtain consent as a lawful basis of processing.[50]

This increase in transparent "worse" practices may also be the result of increased consumer awareness of the term "tracking," because of its recent prominent inclusion in app stores under Apple privacy nutrition labels[51] and Google safety sections.[52] In addition, passage of the CPRA amendments with a focus on "cross-context behavioral advertising" may have further clarified the practice of third-party tracking for companies, resulting in previously "better" practices being updated to "worse" practices to appropriately reflect the new changes in state legislation. Therefore, our data indicates that a small percentage of companies are updating their privacy policies to switch from better to worse third-party tracking practices to comply with the new CCPA requirements, but not also updating their practice of selling data at the same rate. This indicates a knowledge gap where companies are not considering the practice of third-party tracking as a data monetization method that requires them to disclose they also sell data.

Track Users Evaluation Question

The Track Users evaluation question indicates whether the product allows a third-party company to use cookies or other tracking technologies, or whether it otherwise enables a third party to display advertisements to the product's users on other apps and services across the Internet. A company should not track users to target them with advertisements on other third-party websites or services. A user's personal information provided to a product should not be used by a third party to persistently track that user's behavioral actions over time and across the Internet on other apps and services for commercial purposes.[53,54,55,56,57] A "better" response to this evaluation question indicates that the company *does not* allow third-party companies to track users over time and across the Internet on other apps and services. A "worse" response indicates that the company *does* allow third-party companies to track users over time and across the Internet on other apps and services. An "unclear" response indicates that no relevant disclosure is made available in the policies.

Figure 3: Track Users: Do the policies clearly indicate whether or not a user's information is used to track users and display personalized advertisements on other third-party websites or services?

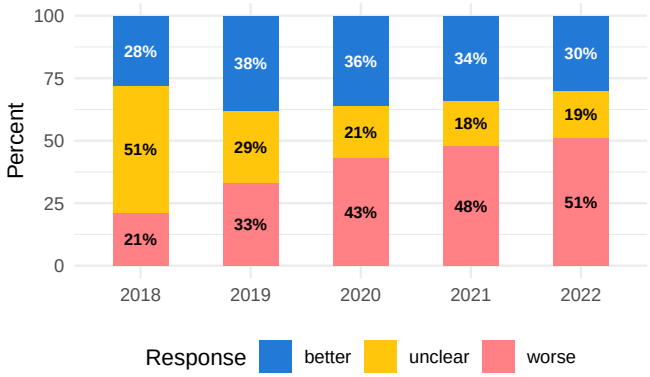


Figure 3 indicates an increase in tracking users across the Internet for commercial purposes since 2021. We see a small decrease, from 34% to 30%, in companies disclosing the "better" practice that they do not use personal information for third-party tracking purposes. However, there remains little to no significant change in the 18% to 19% of companies that still do not disclose whether they engage in the practice of tracking users. The decrease in better practices unfortunately results in a similar increase from 48% to 51% of companies updating their privacy policies to now disclose that they engage in tracking users for commercial purposes. Similar to the increase of third-party tracking, the Track Users data indicates that a small percentage of companies are updating their privacy policies to switch from better to worse third-party tracking practices to comply with the new CCPA requirements, but not updating the practice of selling data at the same rate. This indicates a knowledge gap where companies are not considering the practice of tracking users for commercial purposes as a data monetization method that requires them to disclose they also sell data.

Ad Profile Evaluation Question

The Ad Profile evaluation question indicates whether or not a product creates an advertising profile or allows third-party companies to use cookies or other tracking technologies on the product that would enable those third-party companies to create a behavioral profile or audience segmentation about a user based on the user's personal information, preferences, and characteristics

[50] *See* Information Commissioner's Office (ICO), Legitimate interests, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests.

[51] Apple. (2022, February 9). About privacy information on the App Store and the choices you have to control your data. https://support.apple.com/en-us/HT211970.

[52] *See* Google Play Help, "Understand App Privacy & Security Practices with Google Play's Data Safety" section, https://support.google.com/googleplay/answer/11416267; *See also* Google Play Console Help, "Provide Information for Google Play's Data Safety" section, https://support.google.com/googleplay/androiddeveloper/answer/10787469.

[53] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

[54] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.1.

[55] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(1)(B).

[56] *See* California Privacy Rights for Minors in the Digital World, Cal. B.&P. Code §§ 22580-22582.

[57] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(e)(4), (k), (ah), (aj).

for advertising or marketing purposes across the Internet. A company should not create advertising profiles or allow third parties to use a user's data to create a profile, engage in data enhancement or social advertising, or target advertising based on that profile. Automated decision making, including the creation of ad profiles for tracking or advertising purposes, can lead to an increased risk of harmful outcomes that may disproportionately and significantly affect children or students.[58,59,60,61,62,63] A "better" response to this evaluation question indicates that the company *does not* allow third-party companies to create or use a behavioral profile of any user. A "worse" response indicates that the company *does* allow third-party companies to create or use a behavioral profile of any user. An "unclear" response indicates that no relevant disclosure is made available in the policies.

Figure 4: Ad Profile: Do the policies clearly indicate whether or not the company allows third parties to use a user's data to create an automated profile or engage in data enhancement for the purposes of personalized advertising?

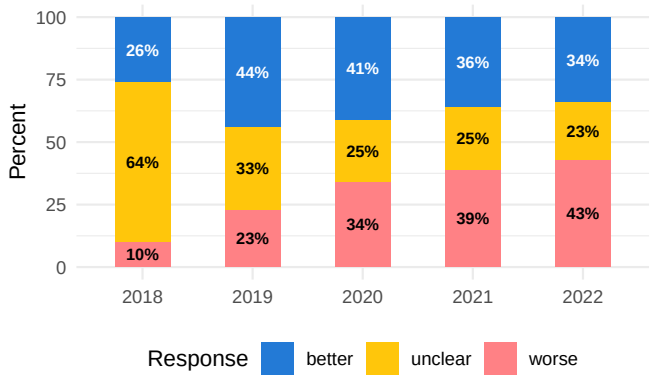


Figure 4 indicates an increase in companies disclosing that they are creating or sharing behavioral profiles of users for commercial purposes since 2021. We see a small decrease from 36% to 34% of companies disclosing the better practice that they do not use personal information for third-party tracking purposes. However, there was also a small decrease, from 25% to 23%, in companies that still do not disclose whether they engage in the practice of creating behavioral profiles. The decrease in better practices and the decrease in remaining non-transparent or "unclear" unfortunately results in an increase, from 39% to 43%, in companies updating their privacy policies to disclose that they engage in creating behavioral profiles of users for commercial purposes that includes targeted advertising. Similar to the increase in third-party tracking and tracking users, the data indicates that a small percentage of companies are updating their privacy policies to switch from better and unclear to worse advertising profile practices in order to comply with the new CCPA requirements. However, these same companies are not updating the practice of selling data at the same rate. This indicates a knowledge gap where companies are not considering the practice of creating advertising profiles of users for commercial purposes as a data monetization method that requires them to disclose that they also sell data.

[58] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

[59] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(b)(2), 22584(e)(2).

[60] *See* California Privacy Rights for Minors in the Digital World, Cal. B.&P. Code §§ 22580-22582.

[61] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140(e)(4), (v)(1)(K), (z), (aj).

[62] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.8.

[63] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code §§ 22584(b)(4)(E)(i), 22584(b)(4)(E)(ii).

Selling Data Multiple Privacy Practice Comparison

The multiple privacy practice comparison explores the privacy practices of a product at the intersection of multiple issues used in our rating criteria. For example, consider a product that discloses they do not sell data to third parties, but also discloses that the product engages in other data monetization methods that would meet the definition of "selling or sharing" data under the CPRA amendments such as using third-party tracking technologies, tracking users across the internet for commercial purposes, or creating advertising profiles for commercial purposes. This multivariable analysis is critically important to help illustrate the complex compliance requirements of selling data and how companies may be in compliance with one variable or practice, but not other practices under the CCPA when you consider additional data monetization methods.

Data Sold: "Better"

The practice of monetizing users' personal information by selling data to third parties is a complex and evolving privacy issue. The passage of recent state consumer privacy protection laws enable consumers to opt out of a company selling their data, but the definition of what selling data means for companies was expanded to include the use of data monetization practices such as third-party tracking and profiling technologies. Table 3 indicates for the 143 companies that disclose in their policies that they do not *Sell Data* to third parties, labeled as "better," whether they also disclose other problematic privacy practices that could be considered monetizing users' data for monetary or other valuable consideration, labeled as "worse." Three additional rating criteria questions are filtered below: the use of **Third-Party Tracking** technologies, **Tracking Users** on

other applications and services across the internet, and creating **Ad Profiles** of users for commercial purposes.

Table 3: Sell Data better vs. Third-Party Tracking vs. Track Users vs. Data Profile 2022. Row coloring indicates the expected "Sell Data" disclosure after the CPRA comes into effect Blue indicates a "better" disclosure, orange indicates "unclear" but likely "worse," and red indicates "worse."

Third-Party Tracking	Track Users	Ad Profile	count
better	better	better	50
unclear	unclear	unclear	15
unclear	unclear	better	1
unclear	better	better	1
better	unclear	unclear	1
better	better	unclear	1
worse	worse	worse	44
worse	worse	unclear	6
worse	worse	better	6
worse	unclear	worse	3
worse	unclear	unclear	6
worse	unclear	better	2
worse	better	worse	2
worse	better	unclear	2
worse	better	better	2
unclear	worse	worse	1
unclear	worse	better	2

We are encouraged that 34% (50/143) of the 143 products that disclose they do not sell a user's data, highlighted in *blue*, also disclose they do not use third-party tracking technologies, and do not track users across the internet, and do not create advertising profiles for commercial purposes. However, 52% (74/143) of companies that disclose they do not sell data, highlighted in *red*, still engage in one or more data monetization practices such as *Third-Party Tracking*, or *Track Users*, or *Ad Profile*, which would be considered selling data under the definition of cross-context behavioral advertising under the CPRA amendments. In addition, the approximate 13% (19/143) of companies that disclose that they do not sell users' data, highlighted in *yellow*, but are non-transparent about use of one or more practices such as third-party tracking technologies, tracking users, or ad profiles are assumed to engage in "worse" practices. These results show that 65% (93/143) of companies that disclose they do not sell data, highlighted in *red* and *yellow*, still engage in one or more data monetization practices or are "unclear." This assumption is based on the *Sell Data* evaluation question data over the long term that indicates when companies update their unclear policies to disclose whether or not they sell data, those disclosures are more likely qualitatively "worse."

Companies are required under the CCPA to incorporate the use of third-party tracking technologies, tracking users across the internet, and creating advertising profiles for commercial purposes into their disclosure of "selling or sharing" a consumer's data to third parties in exchange for monetary value or other valuable consideration. As a result, our data indicates there should be a significant shift in the industry with the percentage of companies that change their policies to disclose they now sell users' data under the CPRA's amendments. The changes related to selling data are expected to be a monumental shift in the industry in 2023 and beyond, with companies required to update their policies with more transparency to come into compliance by disclosing the selling or sharing of their users' data. Our data indicates the industry has so far chosen to simply ignore the changes in the definition of selling or sharing data in response to the CPRA's amendments and continue *Third-Party tracking*, *Track Users*, and *Ad Profile* practices on their products while claiming ignorance in their privacy policies that they "do not sell data." Companies that already say they sell data are not likely to change their "worse" practices or policies regarding the sale of data, but they may increase their transparency on sharing data with the use of tracking technologies and advertising profiles for commercial purposes that are now considered a "sale or share" under the CPRA.

An estimated 65% of companies that disclose they do not sell data engage in one or more data monetization practices.

The industry will likely continue to use tracking technologies in their products to monetize user data, but may update their privacy policy to say they now sell data and still use tracking technologies and advertising profiles for commercial purposes. It is also likely that companies will update privacy policies along with multiple changes that happen to include the change that they now sell users' data without many consumers being aware of this. For example, we evaluated [64] Netflix's privacy policy [65] dated November 2, 2021, which disclosed *"We do not sell personal information,"* but was later updated on November 1, 2022—before the CPRA amendments came into effect—to completely switch practices and now disclose they sell users' data: *"As of the date of this Privacy Notice, we may use certain types of information to offer members an ad supported subscription plan or engage in certain marketing activities. Under the CCPA, this activity may be considered 'selling' or 'sharing.'"* This example is complex, because Netflix chose to introduce a new behavioral advertising-supported subscription plan before the

[64] *See* Common Sense Privacy Evaluation of Netflix, https://privacy.commonsense.org/evaluation/Netflix.

[65] *See* Netflix Privacy Policy, https://help.netflix.com/en/legal/privacy.

CPRA went into effect, and its new selling data disclosure relates only to the new ad-supported plan but not its other paid subscription plans. This may confuse users who are not subscribed to the ad-supported plan; they could assume from this disclosure that their data is not sold, when in actuality, it is.

Even if consumers receive notice of policy changes with privacy policy update emails or pop-up notifications, they may not understand what the changes mean. Often, when consumers learn that the companies and brands they trust switch their historical practices from "we will never sell your data" to "yes, we sell your data" to reflect their already existing practices, there will likely be product or brand reputational damage, as well as consumer confusion over the change in disclosure and lost revenue for companies as consumers lose trust. Consumers are increasingly concerned about their privacy, and they fundamentally understand that "selling data" means companies make money from various methods that include tracking their activities on the product and selling their data to third-party data brokers and companies for advertising purposes, even when consumers pay high subscription fees.[66] Consumers are likely to stop paying to use products that continue to charge higher subscription fees every year and also sell their data to third parties. This "double dipping" approach of charging customers and also monetizing their data goes against the common narrative that "if you are not paying for the product, then you are the product." Increasingly, consumers are paying premium prices or subscription fees to use their favorite apps and services, all while their data is also being monetized, which means the costs outweigh the benefits.

Consumers are learning that even when they are paying a premium for the product, they are also the product.

In their policies, companies claim the definition of "sell" under the CCPA is too broad or unclear, which we discuss further in the *Examples of Selling Data Disclosures* section below. This is similar to how companies historically argued that the industry cannot agree on how to respond to Do Not Track (DNT) Response requests.[67] We expect that companies may conflate the passage of multiple state consumer privacy laws and regulatory inconsistencies in their policy changes that say they now sell data. However, there may be pushback from consumers against companies that now say they now sell consumer data but disagree with what selling means, in an attempt to redirect blame onto confusing privacy laws rather than their own data monetization practices. We have already seen companies take a minimum privacy compliance approach where they conspicuously claim they are not selling data of users identified as children or students, but later disclose that they are selling data of other users such as consumers, parents, and educators of the product as shown in the *Examples of Selling Data Discloses* section below. A consumer might reasonably conclude that any time a company says clearly that they do not sell children's or student's' data that the company does, in fact, sell other users' personal data. The CPRA's expansion of the definition of selling data is generally understood by consumers to more closely align with their awareness and expectations of what selling data actually means, rather than how companies use various technologies and methods to make money from users' data. Ultimately, the different methods of data monetization or exceptions to sale or share are not important to consumers—they just want to know if the product is making money from their data.

Data Sold: "Worse"

Table 4 indicates whether, for the 31 products that disclose the qualitatively "worse" practice that they do sell data to third parties, the company also discloses privacy practices that could be considered monetizing users' data for monetary or other valuable consideration under the CCPA, labeled as "worse" in the table. Three additional rating criteria questions are filtered below: *Third-Party Tracking* technologies, *Tracking Users* on other applications and services across the internet, and creating *Ad Profiles* for advertising purposes.

Table 4: Sell Data worse vs. Third-Party Tracking vs. Track Users vs. Data Profile 2022. Row coloring indicates the expected "Sell Data" disclosure after the CPRA comes into effect. Blue indicates a "better" disclosure, orange indicates "unclear" but likely "worse," and red indicates "worse."

Third-Party Tracking	Track Users	Ad Profile	count
worse	worse	worse	24
worse	worse	unclear	3
worse	worse	better	1
worse	unclear	worse	1
unclear	unclear	unclear	1
better	better	better	1

It is not surprising that 77% (24/31) of the 31 companies that disclose they do sell a user's data, highlighted in *red*, also disclose that they use third-party tracking technologies, track users across the internet, and create

[66] *See* Pew Research Center, Nov. 2019, Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-ResearchCenter_PI_2019.11.15_Privacy_FINAL.pdf.

[67] Some browsers have incorporated "Do Not Track" (DNT) features that can send a signal to the websites you visit indicating you do not wish to be tracked. Because there is not a common understanding of how to interpret the DNT signal, our Site does not currently respond to browser DNT signals.

advertising profiles for commercial purposes. As discussed, these additional monetization practices are all considered selling data with cross-context behavioral advertising under the CPRA amendments to the CCPA. Companies that disclose they sell data but are "unclear" about the use of third-party tracking technologies, tracking users, or creating ad profiles are assumed to also engage in these "worse" practices.

Data Sold: "Unclear"

Table 5 indicates whether, for the 24 products that do not transparently disclose either the qualitatively "better" or "worse" practice that they do or do not sell data to third parties, the company also discloses privacy practices that could be considered monetizing users' data for monetary or other valuable consideration under the CPRA amendments, labeled as "worse." Three additional rating criteria questions are filtered below: *Third-Party Tracking* technologies, *Tracking Users* on other applications and services across the internet, and creating *Ad Profiles* for commercial purposes.

Table 5: Sell Data unclear vs. Third-Party Tracking vs. Track Users vs. Data Profile 2022. Row coloring indicates the expected "Sell Data" disclosure after the CPRA comes into effect. Blue indicates a "better" disclosure, orange indicates "unclear" but likely "worse," and red indicates "worse."

Third-Party Tracking	Track Users	Ad Profile	count
unclear	unclear	unclear	5
unclear	better	unclear	1
worse	worse	worse	9
worse	worse	unclear	4
worse	worse	better	1
worse	unclear	worse	2
worse	unclear	unclear	1
unclear	worse	worse	1

Approximately 75% (18/24) of the 24 products that do not disclose whether they sell a user's data, highlighted in *red*, do disclose either that they use third-party tracking technologies, track users across the internet, or create advertising profiles for commercial purposes. Companies likely do not consider their third-party tracking or advertising practices the same practice as selling a user's personal information to third parties. Companies may think they are simply making money by providing *access* to their product for third parties with their users' automatically collected personal information, which is why they remain unclear about selling data. As discussed, there is a higher awareness among consumers about the practice of explicitly selling data, which may indicate why companies remain "unclear" or non-transparent on the practice—they don't want to risk losing current users, subscription revenue, or future app downloads. However, these companies still disclose the practice of using third-party tracking technologies, tracking users on other sites and services across the internet, or creating advertising profiles for commercial purposes. As discussed, these additional monetization practices are also considered selling or sharing data with cross-context behavioral advertising under the CPRA amendments, but companies are not in compliance. Based on historical trends and on this analysis, companies that do not say whether or not they sell data and are "unclear" or non-transparent about the use of third-party tracking technologies, tracking users, or creating ad profiles can be reasonably assumed to be selling users' data and engaging in these "worse" data monetization practices.

Examples of Selling Data Disclosures

Our results indicate a majority of companies (73%) currently disclose the "better" practice that they do not sell users' data to third parties, but they have other data monetization practices that would be considered selling or sharing data under the CCPA. As companies updated their privacy policies in 2022 to disclose whether or not they sell users' data to third parties, we identified several different types of policy disclosures related to how companies describe the practice of selling data. The following categories illustrate the different approaches our reviewers identified in how companies choose to disclose the practice of selling data in their policies:

Transparently Better

We see a minority of companies (~20%) with policies that consistently and transparently disclose they do not sell users' data, and that also transparently disclose they do not engage in other data monetization methods such as third-party tracking, targeted advertising, or profiling, which is consistent with the CPRA's definition of selling or sharing data. These companies earn our highest blue "Pass" privacy rating[68] because they do not engage in any forms of data monetization and typically earn revenue through the sale of hardware, paid monthly subscriptions, paid app downloads, in-app purchases, or license fees. For example, we evaluated[69] Apple Siri's privacy policy[70], which says, *"Apple does not sell your personal*

[68] *See* Common Sense Media, Privacy Ratings, https://privacy.commonsense.org/resource/privacy-ratings.

[69] *See* Common Sense Privacy Evaluation of Apple Siri, https://privacy.commonsense.org/evaluation/Apple-Siri.

[70] Apple, Privacy Policy, https://www.apple.com/legal/privacy/en-ww (Accessed April 1, 2023).

data including as 'sale' is defined in Nevada and California. Apple also does not 'share' your personal data as that term is defined in California."

Transparently Worse

We see a small percentage of companies consistently and transparently disclose they sell users' data (~16%), and also transparently disclose they engage in other data monetization methods, such as third-party tracking and targeted advertising, which are consistent with the CPRA's definition of selling or sharing data. These companies are clear and honest about their data monetization practices, and we find they typically begin their privacy policy by saying they respect and value the privacy of their users. These companies are in compliance with the CPRA amendments, but they are in the minority within the industry. Our research shows most other companies in the industry are not in compliance with the CPRA with respect to disclosing their data selling practices, which puts transparently "worse" companies at a competitive disadvantage in the marketplace. For example, we evaluated [71] Roku's supplemental "Your Privacy Choices" [72] policy, which says *"We disclose personal information as described in our privacy policy for different purposes, including to bring you more relevant ads, help you discover content, and provide a more tailored experience to you on our services. Some of these disclosures may be considered a 'sharing' of personal information for 'cross-context behavioral advertising' or 'targeted advertising,' or a 'sale' of personal information under relevant law."*

Disagreement

We see a minority of companies updating their policies in 2023 to transparently switch practices from historically saying they will never sell data to now disclosing they do sell data, but the policy change is made with contradicting language that is difficult to understand because the company disagrees with the CPRA definition of selling data.. Change is hard, and these policy changes often say the definition of "sale" and "share" is too broad and not within the commonly understood meaning of exchanging data for money, but it's not clear to consumers with these policy changes whether or not the company actually sells their data. For example, we evaluated [73] ABCMouse's privacy policy [74], which says, *"[W]e will never monetize the PI of any User of the Services by providing it to a third party in exchange for money. The CCPA has a broader definition of the term 'sell' which includes disclosing PI to any third party for valuable consideration. When we work with our advertising partners, we are disclosing certain information such as cookies for their services, which are of value to us. You may be entitled to direct us to stop disclosing your PI to third parties for monetary or other valuable consideration."*

Confusion

Many companies say they don't sell data, but confusingly still offer the ability for users to opt out of sale, which implies they do sell data. They sometimes also state factual inaccuracies in their policies about the CCPA in their attempt to understand how the practice of selling data applies to their own privacy practices. For example, we evaluated [75] the gaming company Storm8's privacy policy [76], which says, *"The California Consumer Protection Act ('CCPA') requires us to disclose categories of personal information sold to third parties and how to opt out of such sales. The CCPA defines personal information to include online identifiers, including IP address, cookies, and mobile IDs. The law also defines a 'sale' to include simply making data available to third parties. We let advertising and analytics providers collect IP addresses, cookie IDs, mobile IDs through our sites and apps when you use our online services, and they may further 'sell' such information, but we do not 'sell' any other types of personal information. If you do not wish for us or our partners to 'sell' or further 'sell' your personal information to third parties for advertising or analytics purposes, you can make your Do Not Sell Request by opting out of third-party tracking as described in this Cookie section."* This type of confusion about selling data is quite common. First, the CCPA does not define selling or sharing as simply making data available to third parties. Second, the company is confused into thinking third-party advertising companies are the ones selling their users' data, but that they are not selling data because they don't sell other types of user data to those same third parties. Lastly, the company makes the contradictory statement that users can opt out of selling their data from both Storm8 and their "partners," including some types of personal information but not other types of personal information. This can be confusing to consumers.

Inconsistencies

We see far too many companies still transparently disclosing they do not sell their users' data, but also inconsistently disclosing that they sell or share data in supplemental policies or that they engage in other data monetization methods such as third-party tracking, profiling, and third-party targeted advertising of their users, which would satisfy the requirement of selling or sharing

[71] *See* Common Sense Privacy Evaluation of Roku, https://privacy.commonsense.org/evaluation/Roku.

[72] Roku, Your Privacy Choices, https://privacy.roku.com/ccpa (Accessed April 1, 2023).

[73] *See* Common Sense Privacy Evaluation of ABCMouse, https://privacy.commonsense.org/evaluation/ABCmouse.com.

[74] *See* ABCMouse, Privacy Policy, https://www.abcmouse.com/abc/privacy/current (Accessed April 1, 2023).

[75] *See* Common Sense Privacy Evaluation for Property Brothers Home Design, https://privacy.commonsense.org/evaluation/property-brothers-home-design.

[76] Storm8, Privacy Policy, https://www.storm8.com/notice-of-privacy (Accessed April 1, 2023).

data under the CPRA. These companies typically market themselves prominently as privacy-protecting products that "care about your privacy" and that would never sell their users' data to third parties for profit, but they still share data for personalized advertising. There is also likely confusion about whether monetizing a user's data with the first-party company is a sale under the CCPA, or only if data is shared with a third party, or if sharing data with partners, affiliates, or service providers constitutes a sale depending on if they are categorized as first party or third party. Whether intentional or not, these companies are falsely disclosing that they do not sell their users' data. As a result, these products give children, students, parents, and educators a false sense of privacy and safety because they market their product as more privacy-protecting than it really is by disclosing that they don't sell data but only share it for cross-context behavioral advertising. This practice does not give users appropriate or adequate notice about their data monetization practices, so users cannot provide informed consent.

For example, we evaluated [77] Amazon's Privacy Policy [78], which says that a user's personal information is not sold or rented to third parties: *"Information about our customers is an important part of our business, and we are not in the business of selling our customers' personal information to others."* In addition, Amazon's policy discloses: *"No sale of personal information. In the twelve months prior to the effective date of this Disclosure, Amazon has not sold any personal information of consumers, as those terms are defined under the California Privacy Rights Act."* However, Amazon's "Additional State-Specific Privacy Disclosures" [79] policy inconsistently says they share a list of categories of customer's personal information for cross-context behavioral advertising: *"Any personal information Amazon may have shared for the purpose of cross-context behavioral advertising, as that term is defined by the California Privacy Rights Act, in the twelve months prior to the effective date of this Disclosure falls into the following categories..."*. Amazon states that they do not sell data in their policy and then later provides the detail that they share data only for monetary value under the CCPA.

Companies know that consumers are more likely to make a decision not to use a product that discloses they sell their data, but consumers may have fewer concerns with products that say they only share but not sell data. Therefore it is not surprising that companies have adopted methods of disclosure that enable them to claim they are privacy-protecting because they only share data, but do not sell as defined under the CCPA. Similarly, Microsoft's "U.S. State Data Privacy Laws Notice" [80] states that they "share" personal information with third parties for personalized advertising purposes—which is a form of data monetization—but Microsoft also discloses they do not sell personal information.

In another example, we evaluated [81] Meta's "Privacy Policy" [82] and "About Facebook Ads" page, [83] which says, *"We don't sell any of your information to anyone, and we never will."* In addition, Meta's supplemental "United States Regional Privacy Notice" [84] says, *"We don't 'share' your Personal Information, as defined in the California Consumer Privacy Act ('CCPA'). We also don't sell any of your Personal Information, and we never will."* Being a social media company, Meta's disclosure that they do not sell or share data under the CCPA is counterintuitive, because by design the entire business model of Meta and similar social media companies is built on the monetization of users' behavioral data for tracking and personalized advertising.

Lastly, we evaluated [85] AI company Midjourney's Privacy Policy [86], which says, "*Midjourney does not sell Your Personal Information, as defined under CCPA. If in the future we do sell your personal information, we will notify you and you may have the right to opt out of such sale.*" This type of inconsistent language, and the disclosure that a consumer has the right to opt out of sale, is confusing because it provides no expectation of a company's privacy practices if they can change their most important practices at any time, and for any reason. If a company promises they will not sell data until they decide to change their mind in the future, then there can be no consumer trust in how that company will collect and use their personal information. This type of disclosure may also be an attempt by companies to claim that they provide notice of a consumer's rights to opt out of sale under the CCPA regardless of whether they sell data, which actually may be more confusing because it is less clear to consumers what a company's actual practices are when they disclose that they do not sell data but also that they will provide the ability to opt out of sale.

Companies may also explicitly reserve the right to sell data in the future as a potential monetization strategy, which should be interpreted by consumers that the company does sell their data. Companies that reserve the

[77] *See* Common Sense Privacy Evaluation for Amazon Alexa, https://privacy.commonsense.org/evaluation/Amazon-Alexa.

[78] Amazon, Privacy Policy, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496 (Accessed April 1, 2023).

[79] *See* Amazon, Additional State-Specific Privacy Disclosures, https://www.amazon.com/gp/help/customer/display.html?nodeId=GC5HB5DVMU5Y8C (Accessed April 1, 2023).

[80] *See* Microsoft, U.S. State Data Privacy Laws Notice, https://privacy.microsoft.com/en-US/ccpa1 (Accessed April 1, 2023).

[81] *See* Common Sense Privacy Evaluation for Facebook, https://privacy.commonsense.org/evaluation/Facebook.

[82] Meta, Privacy Policy, https://www.facebook.com/privacy/policy (Accessed April 1, 2023).

[83] Facebook, About Facebook Ads, https://www.facebook.com/about/ads (Accessed April 1, 2023).

[84] Meta, United States Regional Privacy Notice About this Notice, https://www.facebook.com/privacy/policies/uso (Accessed April 1, 2023).

[85] *See* Common Sense Privacy Evaluation for Midjourney, https://privacy.commonsense.org/evaluation/Midjourney.

[86] See Midjourney, Privacy Policy, https://docs.midjourney.com/docs/privacy-policy (Accessed April 1, 2023).

right to sell data in the future may also be trying to mitigate potential compliance risks as privacy laws and definitions change.

Obfuscation

We see some companies indirectly disclose the practice of selling data but without using the words "sale" or "sell," so it's difficult for consumers to skim privacy policies looking for keywords to try to understand whether the company sells their data. Also, some companies discuss their data monetization practices in the abstract within the context of "sharing" assets with third parties for personalization or commercial purposes. These disclosures are also typically found in privacy policies right before or after discussions of transferring assets of the company to third parties—which includes personal information from users—in the event of a merger, acquisition, or bankruptcy, which implies that any asset transfer to third parties does not meet the CPRA definition of "sell," because transferring data is an exception to sale.[87] This type of policy language is often difficult to comprehend even for privacy experts, and it ultimately does not provide sufficient notice to parents, educators, or consumers about the company's data selling practices.

For example, we evaluated[88] Bloomberg's privacy policy[89], which says, *"While we do not 'sell' your personal information in exchange for money or 'share' your personal information for cross-context behavioral or targeted advertising outside of the use of electronic technologies to provide relevant advertisements, to the extent that certain practices described above relating to advertising constitute targeted advertising, or are considered 'selling' or 'sharing' under California privacy law, you may adjust your preferences by using the designated tool within Bloomberg's digital properties."* This type of confusing "sandwich" disclosure begins with the "better" statement that the company does not sell data, which is what most consumers are looking for when they do a keyword search in a privacy policy and could reasonably assume as the company's practices. However, the statement has subsequent exceptions for the use of electronic technologies to provide targeted advertising, which allows for the "worse" practice of selling data that applies to all users. The selling data clause then concludes with the "better" statement that opt-out privacy controls and preferences are available in these situations. Unfortunately, this is an all-too-common practice in the industry when describing the practice of selling data. It is not clear to consumers and ultimately does not adequately inform or allow users to provide meaningfully informed consent about whether the company sells or shares data under the CCPA.

Unclear

We still see numerous lesser-known companies that have not updated their policies to disclose whether or not they sell users' data (12%), either because they are still unaware of the CPRA compliance obligations, or because they think just disclosing general statements that they don't collect any data is sufficient to convey they also don't sell data.[90] However, some companies may not understand that simply providing access to their users' data to a third party for their own commercial purposes could be selling data. Therefore, these companies likely prefer to remain non-transparent on the practice of selling data because they do not fully understand the practice, and they also remain non-transparent on other data monetization methods in the hope that users assume that because they do not discuss selling data, they must be more privacy-protecting than they really are.

Companies may incorrectly assume that users do not expect to see all the possible practices, or lack thereof, of a product in its privacy policy because they assume that like a nutrition label, listing all of the ingredients a product does and *does not* contain would be too much information. However, privacy policies and nutrition labels for products are not the same. If a product's nutrition label does not disclose that it contains a potentially harmful ingredient that consumers look for when making a decision on whether to purchase the product, such as wheat, dairy, or nuts, that should mean that the product *does not* contain those potentially harmful ingredients and therefore the product does not pose a risk for that particular consumer.

Unlike a product's nutrition label, a company's privacy policy that is unclear or non-transparent regarding a privacy practice means the product may still engage in that practice without providing any additional notice.

Even more problematic is when companies cannot agree on a standard definition of what an ingredient actually contains, or on the ingredient's origin, and may use multisyllabic and confusing names to describe ingredients. We see similar issues in the privacy landscape with obfuscating language, and in some cases we see a lack of vocabulary and societal awareness necessary to discuss issues in a consistent manner. This lack of consensus results in the use of different language to explain similar privacy practices, which further confuses consumers. A product's privacy policy that does not transparently

[87] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.140(ad)(2)(C), (ah)(2)(C); *See also* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code § 22575(b)(5).

[88] *See* Common Sense Privacy Evaluation for Bloomberg, https://privacy.commonsense.org/evaluation/Bloomberg-Business-News.

[89] *See* Bloomberg, Privacy Policy, https://www.bloomberg.com/notices/privacy (Accessed April 1, 2023).

[90] *See* Clipish, https://www.clipish.info/privacy ("The world's smallest privacy policy") (Accessed April 1, 2023).

disclose its "worse" practices, which consumers look for when making a decision to use the product, means the product should not be presumed safe, because the product still reserves the right to engage in the "worse" practices without any notice, putting users at risk for potential harm.

Regardless, for food labeling, some ingredients are so harmful to some people that top allergens are often explicitly disclosed for clarity (e.g., Contains: Nuts, Dairy, Wheat, Soy). Many privacy issues pose similar risks and should be explicitly disclosed, regardless of whether or not a company engages in such a practice.

California Only

Unfortunately, many companies disclose that the right to opt out of sale under the CCPA is available only to users of their product in the state of California. This means that the company excludes California users' data from sale, but sells every other user's data regardless of jurisdiction. These types of companies allow only the users who are residents of the state of California to opt out of sale once they prove residency. Every other user of the product in a U.S. state other than California, or located in another country outside the European Union, is not provided the same privacy rights. This is similar to the "Limited Protections" scenario discussed below, where only some users, such as children and students, receive stronger privacy protections. Rather than simply applying the same CCPA privacy rights to opt out of sale or sharing to all of a product's users, the company provides only the minimum amount of privacy rights to the minimum number of users, which is not a privacy-protecting best practice. Counterintuitively, however, this approach is likely to actually increase a company's privacy compliance and transactional costs.

There are already several U.S states with similar privacy laws modeled after the CCPA, including Colorado, Connecticut, Iowa, Nevada, Utah, and Virginia.[91] However, many companies do not also have a supplemental privacy policy for each of these additional states to determine which different privacy practices apply to which users in which states. For example, Meta's supplemental "United States Regional Privacy Notice"[92] says, "*This Notice explains how we collect, use, and disclose your Personal Information. It also describes how to exercise your rights under the California Consumer Privacy Act, the Colorado Privacy Act, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act. We call those laws collectively the 'U.S. Privacy Laws.'*" Therefore, companies are likely to simply add new state consumer privacy laws to the same supplemental policy and use the U.S state with the broadest and strongest consumer privacy law—typically California's CCPA—as the highest bar applied to all other state consumer privacy laws in order to avoid differences in statutory and regulatory definitions and ensure compliance.

Limited Protections

Some companies with products for a mixed audience that includes children, students, parents, educators, and consumers transparently disclose they do not sell the data of kids or students, but also transparently disclose that they *do* sell the data of other users such as parents, educators, and consumers. This mixed-user example often sends mixed messages that the product appears safer for the privacy of all users than it actually is. Some companies prominently disclose only that they don't sell kids' data—which is a prohibited practice anyway under the CCPA[93]. This implies that the company also does not sell data generally when there is no other affirmative disclosure that they do or do not sell data of other users. For example, we evaluated[94] HBO Max's privacy policy[95], which says: *"We do not sell personal information from Kids Profiles,"* but provides no other disclosures related to selling data in its privacy policy. Consumers would only learn that HBO Max sells other users' data if they also read the "California and Other US States Rights"[96] policy, which says: *"We may collect, share, sell, or otherwise process these categories of personal information, including Sensitive Personal Information, for the following business or commercial purposes."* In another example, we evaluated[97] Disney's privacy policy[98], which does not disclose anything about their practice of selling users' data, but Disney's "Your California Privacy Rights"[99] supplemental policy does say: *"We do not sell personal information of known minors under 16 years of age."* However, Disney's "Your California Privacy Rights" policy also says that *"As the term is defined by the CCPA, we 'sold' the following categories of personal information in the last 12 months..."*.

In addition, many companies do not disclose their data selling practices in their privacy policy where consumers would expect to find it, but rather only in a supplemental "California Privacy Rights" or "State Privacy Notice"

[91] IAPP, US State Privacy Legislation Tracker, https://iapp.org/resources/article/us-state-privacy-legislation-tracker.

[92] Meta, United States Regional Privacy Notice, https://www.facebook.com/privacy/policies/uso (Accessed April 1, 2023).

[93] *See* California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.120(c).

[94] *See* Common Sense Privacy Evaluation for HBO Max, https://privacy.commonsense.org/evaluation/HBO-Max.

[95] *See* HBO Max, Privacy Policy, https://www.hbomax.com/privacy/en-emea (Accessed April 1, 2023).

[96] *See* HBO Max, California and Other US States Rights, https://www.hbomax.com/privacy/usrights/en-us (Accessed April 1, 2023).

[97] *See* Common Sense Privacy Evaluation for Disney, https://privacy.commonsense.org/evaluation/Disney.

[98] *See* Disney, Privacy Policy, https://www.disneyplus.com/legal/privacy-policy (Accessed April 1, 2023).

[99] *See* Disney, Your California Privacy Rights, https://www.disneyplus.com/legal/your-california-privacy-rights (Accessed April 1, 2023).

policy, which is more difficult for users to find because they may not be aware of the association of selling data with "California" or "U.S States." For example, Disney's privacy policy [100] does not disclose anything about their practice of selling data, which is where the majority of consumers looking for that information would expect it to be found. Rather, Disney only describes its data selling practices in its supplemental "Your California Privacy Rights" [101] policy.

Notice in privacy policies about the practice of selling data is required to be disclosed under the CPRA's regulations and must be easy to read and understandable to consumers. [102] Privacy policies need to be easy to find and use plain, straightforward language that is easy to understand and avoid technical or legal jargon. However, from the examples provided above, it is extremely difficult for an average consumer to understand whether a company is selling their data.

The Common Sense "Warning" privacy rating flags the use of any collected data for commercial purposes (such as selling data or displaying targeted ads) from any user. We do not make the distinction between stronger privacy protections given to children or students vs. weaker privacy protections for other users such as parents and educators. Privacy policies rarely disclose if privacy protections change when a child user becomes a teen or adult user, or a student user becomes a teacher user. In mixed-privacy environments, as children under 13 become teens, and teens under 18 become adults, the privacy practices related to their data would automatically change to worse practices. As a result, companies could use previously collected data, without further notice or consent, in different contexts than those agreed to when the data was collected. Alternatively, inferences from a parent user's account can be linked to a child user's behavior to indirectly target advertisements to the child through the parent, or with student data provided through a teacher account. Consumers, parents, and educators all use privacy ratings to make informed decisions to use the product themselves as well as with their children and students. Therefore, any privacy practice of a product that puts any user's data at risk is flagged with a "Warning," so any user who is viewing privacy ratings is informed of the risks and has all the information necessary to make an informed decision to use the product.

[100] *See* Disney, Privacy Policy, https://www.disneyplus.com/legal/privacy-policy (Accessed April 1, 2023).

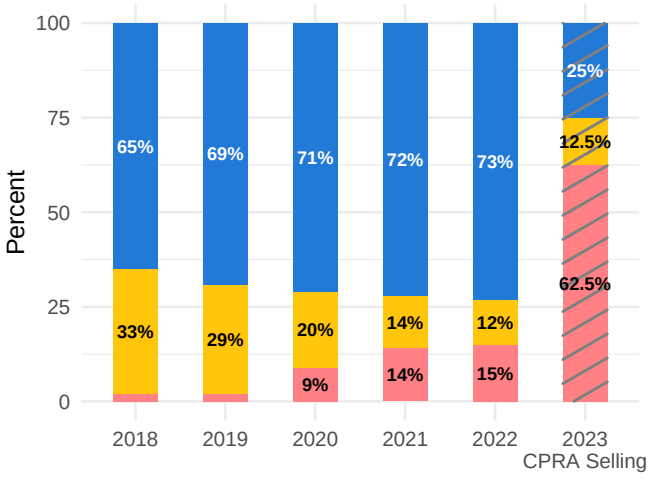
[101] *See* Disney, Your California Privacy Rights, https://www.disneyplus.com/legal/your-california-privacy-rights (Accessed April 1, 2023).

[102] California Consumer Privacy Act Regulations, § 7003, Requirements for Disclosures and Communications to Consumers, https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf; *See also*, California Consumer Privacy Act Regulations, § 7011. Privacy Policy.

Companies Need to Disclose That They Sell Your Data

The majority of companies that currently disclose they do not sell users' data to third parties, but that have other practices that are considered selling data under the new CPRA amendments, are expected to disclose they now sell users' data, which will increase the percentage of companies that sell data significantly, from 16% to at least 62%. Figure 5 indicates that companies are currently disclosing their data-selling practices in a manner that is inconsistent with the requirements of the new CPRA. Therefore, 48% of the industry will need to switch from "better" to "worse" data selling practices in their policies, or risk enforcement from the California Privacy Protection Agency (CPPA) [103] or the Office of the Attorney General. [104] In addition, companies with policies that remain non-transparent on the issue of selling data, and that are also non-transparent on the use of third-party tracking, tracking users, or the creation of ad profiles, are presumed to likely be selling data as supported by our long-term research on this issue. Including the non-transparent or "unclear" products in our analysis is expected to increase the portion of companies that should disclose they sell data under the CCPA from 62% to 75%.

Figure 5: Speculative Sell Data responses in 2022 if industry does not change practices based on current responses to Sell Data, Third-Party Tracking, Track Users, and Data Profile



In addition, the *Sell Data* evaluation question indicates that in 2022, 73% of policies said they don't sell data. However, the previously discussed *Third-Party Tracking* evaluation question indicates that, at most, 27% disclose

[103] State of California, California Privacy Protection Agency (CPPA), https://cppa.ca.gov.

[104] State of California, Department of Justice, Office of the Attorney General, https://oag.ca.gov.

the "better" practice that they do not engage in third-party tracking for commercial purposes and could consistently say they don't sell data. Note that this is a generous interpretation, since 59% explicitly say they allow third-party tracking, while 14% don't explain their third-party tracking practices. From our data, we know that it's extremely unlikely that "better" practices are being used by the majority of the 14% of products that don't clearly disclose their *Third-Party Tracking* practices.

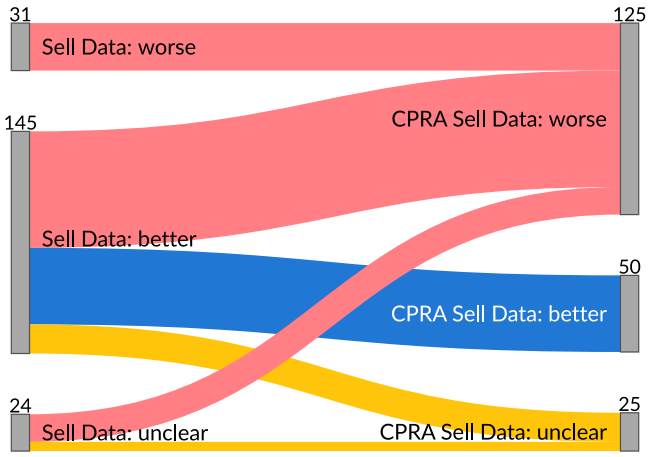
The bottom line is that at least 48% of the industry is not in compliance with the California Consumer Privacy Act (CCPA)'s disclosure requirements for selling data to third parties.

Therefore, if we take a more nuanced look at the 73% of companies that said they don't sell data in 2022, relative to the other practices, we can see what a more realistic interpretation of data-selling practices looks like. After we account for all three of the other practices mentioned above (*Third-Party Tracking*, *Tracking Users*, and *Ad Profiles*), a more accurate interpretation would be that approximately 25% of companies actually don't sell data, that approximately 12% are "unclear" across all practices (or a mix of better and unclear practices), and that a majority 62% of companies should disclose they actually sell data under the CPRA. This is a huge discrepancy between how companies are choosing to discuss their data-selling practices and their obligations to appropriately and accurately disclose those practices. Our previous research indicates it is most likely that the majority—if not all—of the remaining 25 products (approximately 13%) with policies that are either a.) inconsistent, but not explicitly worse, across multiple practices, or b.) that do not provide enough information to determine their actual selling practices, as indicated by "unclear" under the CPRA Sell Data column in table 6, are also likely selling data. That suggests that between 62% and 75% of the industry is selling data in 2023—which means the entire industry is flipped upside down if 73% of companies currently disclose they *don't* sell data under the CCPA. Figure 6 attempts to further illustrate the inconsistency in policy disclosures with respect to practices around selling data as defined by the CPRA.

Table 6: 2022 Sell Data privacy policy disclosures as compared to what CPRA Sell Data disclosures should be.

Sell Data	CPRA Sell Data	Products
worse	worse	31
unclear	worse	18
unclear	unclear	6
better	worse	76
better	unclear	19
better	better	50

Figure 6: Disparity in sharing versus selling approximately 48% (76 + 19)/200 of products evaluated indicate they do not sell data, or are unclear about selling data, but under the CPRA definitions of sell, share, and cross-context behavioral advertising these companies should be disclosing they sell data.



Conclusion

Parents, educators, and consumers are increasingly concerned about their privacy, and they already understand that companies make money by tracking their online activities and selling their data to third-party companies for profit. What's currently unclear for many consumers are the complex and indirect ways that companies go about monetizing their data through third-party tracking, bundling, and profiling personal information and behavior in order to further influence parents', kids', students', and consumers' behavior. When surveyed about privacy, consumers overwhelmingly say, *"I want to have control over what marketers can learn about me online,"* (91%) and *"I would like to understand how digital marketers use the information they collect about my online activities"* (87%).[105] Laws like the CCPA were passed in order to help bring clarity to these practices and force companies to use more plain, understandable, and direct terms in their policies, rather than overly complex, indirect, and confusing language, or technical jargon that works to prevent an understanding of a company's actual practices by the average parent or consumer. Companies need to provide clear and easy-to-understand notice of whether they sell any user's data to third parties for profit.

It's estimated that almost three-quarters of companies currently disclosing that they do not sell consumers' data will either need to change their policies, or they will need to improve their practices to better protect their users' data and privacy.

The CPRA amendments to the CCPA were a good first step toward increasing clarity on what the sale of data means in order to better protect kids and families, who can now make better informed decisions about whether to use products that say they sell kids' data for profit. But we can't stop there. The next step will require holding companies accountable when they don't follow the rules or when they mislead consumers by saying they don't sell data. Companies don't give consumers a meaningful choice or ability to provide consent about whether their data is sold–if companies can say one thing, but do another, which is misleading. It is also unfair and deceptive to parents and caregivers, because it impacts their decision making ability and the practice is not reasonably avoidable if nearly three-quarters of the industry are monetizing data in some way–which is especially concerning given that millions of children are impacted.

Enforcement may come from the Federal Trade Commission (FTC) with jurisdiction over unfair and deceptive trade practices, or under the CCPA with the new California Privacy Protection Agency (CPPA), as well as state attorneys general and local district attorneys. Otherwise, companies will continue to use incomprehensible, hard-to-find language in their policies that is confusing to consumers and that often misleadingly claims to be more protective of privacy than they really are. This ultimately impacts kids' and families' privacy and creates an unfair and deceptive marketplace for everyone.

The Common Sense Privacy Program will continue to provide free privacy ratings of the apps and services that kids and families use every day in order to help parents, educators, and consumers make more informed decisions about which products they are comfortable using. However, to fully protect kids' privacy, we need meaningful consent. To obtain meaningful consent, consumers need to know which companies and products say they sell their data, as well as a stronger, more comprehensive state or federal privacy law that bans the practice of selling data for all users unless separate opt-in consent is explicitly obtained. Without these baseline expectations, the industry will continue to make money by influencing and exploiting kids' and families' data for commercial purposes, all while claiming they respect our privacy.

[105] Americans Can't Consent to Companies' Use of Their Data, Annenberg School for Communication (Feb. 10, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4391134.

About Common Sense

Common Sense is the nation's leading nonprofit organization dedicated to improving the lives of all kids and families by providing the trustworthy information, education, and independent voice they need to thrive in the 21st century. Our independent research is designed to provide parents, educators, health organizations, and policymakers with reliable, independent data on children's use of media and technology and the impact it has on their physical, emotional, social, and intellectual development. For more information, visit privacy.commonsense.org

common sense®

commonsense.org

© 2023 Common Sense Media. This work is licensed under a Creative Commons Attribution 4.0 International Public License. Common Sense, associated names, associated trademarks, and logos are trademarks of Common Sense Media, a 501(c)(3) nonprofit organization, FEIN 41-2024986.

Cover image: © iStock/StefaNikolic

