common sense®

2023

Privacy Program

Evaluation Framework

Credits

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

Suggested citation: Kelly, G., Graham, J., & Garton, S. (2023). *Privacy Program Evaluation Framework*. San Francisco, CA: Common Sense Media

Table of Contents

Foreword

The Privacy Evaluation Framework comprises a series of questions used to rate and compare products on multiple dimensions of privacy, safety, security, and compliance, incorporating criteria based on legal, societal, educational, and child development best practices. The following evaluation questions are used as part of our *Full* privacy evaluation process to generate quantitative overall scores and sub-scores for concern categories. Each individual evaluation question below includes a figure that indicates aggregate responses to our privacy evaluations of companies' privacy policies over the past five years. Most evaluation questions have a "better" or "worse" qualitative component that indicates a more privacy-protecting practice versus a less privacy-protecting practice, respectively. Additionally, we have included a summary paragraph below each evaluation question to provide more context on the type of indicators that are relevant to answering each question. Each evaluation question also displays a privacy practice summary statement that is used to explain when a company engages in a respective better or worse practice, and when indicated, transparency-only statements are displayed if the practice does not have a qualitative component.

Most evaluation questions display relevant citations to statutes or regulations with a parenthetical summary of the citation in order to provide more context for how each particular citation's legal authority applies to its associated evaluation question. Evaluation questions without citations but with "better" or "worse" practice statements are considered industry best practices that companies should still disclose in their privacy policy, because these practices are still important to the product's audiences and are likely to be included in future privacy legislation or regulations. Direct citations are related to the practices described in each evaluation question and include the same terms and language that are used to enforce legal rules, otherwise known as primary legal authority. Indirect citations are not directly related to the practices described in each evaluation question, but may still be used to enforce legal rules, and may be referred to as persuasive legal authority. Indirect citations are indicated by the preceding text "*See*" in each footnote. Indirect citations are included because they clearly support the purpose and scope of the evaluation question, but there is an inferential step between the practices described in the evaluation question as stated and the cited legal authority. For example, an indirect citation may not use the same terms or language as described in an evaluation question, such as the practice of "tracking" users, but an associated indirect citation may still be relevant, because it includes a definition of "personal information," which includes a type of data called "persistent identifiers" that are used to track users. Therefore, the indirect citation is within the scope of the practice described in the evaluation question and related to the cited legal authority.

Each evaluation question's "better" or "worse" qualitative component is determined by the Privacy Program, and is continually informed by academic research, industry standard best practices, consumer surveys, and third-party risk assessment frameworks. Each queston's privacy risk determination considers whether the collection, use, or disclosure of personal information from any user of the product increases or decreases risk based on the respective practice. All of the privacy evaluation questions aim to create a comprehensive assessment of all the issues that a product's privacy policy should disclose that may apply to any user of the product. Therefore, because a practice can happen at any time, and to any user, our qualitative statements summarize the practice by saying that it does or does not happen. This provides easier to understand and actionable information to our audiences to help better understand the potential risks of a product and enable better-informed decisions about whether to use a product, given practices that may have already happened to other users of the product, or that may happen to them depending on the context of how the product is used.

Many evaluation questions do not have a "better" or "worse" qualitative component because they are "complex" and therefore only indicate a "Yes" or "No" response in regard to transparency about the specified practice described in the question. A complex question indicates that it may be, generally speaking, difficult to determine whether a practice is "better" or "worse" in all scenarios. For complex questions, more specific context is necessary, and overall risk may depend on the type of user of the product, or how the product is used, and there may also be an unavoidable practice for the majority of products—such as sharing data—that could increase or decrease risk for the user depending on the purpose for which their data is used.

The full evaluation questions are listed below in the order in which they appear in our evaluation process. This order follows the typical structure of how a privacy policy should disclose what data is collected and how it is used, which also aligns with the Fair Information Practice Principles (FIPPs)[1].

[1] Federal Trade Commission (FTC), Privacy Online: Fair Information Practices in The Electronic Marketplace (May 2000).

[2] Creative Commons, CC by 4.0 Legal Code.

Assessment

0.1.1: Policy Available

Are the privacy policies for the specific product (vs. the company website) made publicly available?

Statutes & Regulations:

- CalOPPA: (An operator of an online service or application that collects personally identifiable information through the Internet about individual consumers from California who use or visit its service is required to conspicuously post a privacy policy.)[3]
- CAADCA: (Companies need to provide privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature.)[4]
- DSA: (Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions.)[5]

[3] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(a).

[4] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(a)(7).

[5] Digital Services Act (Regulation (EU) 2022/2065), Terms and conditions, Art. 14(1), (5).

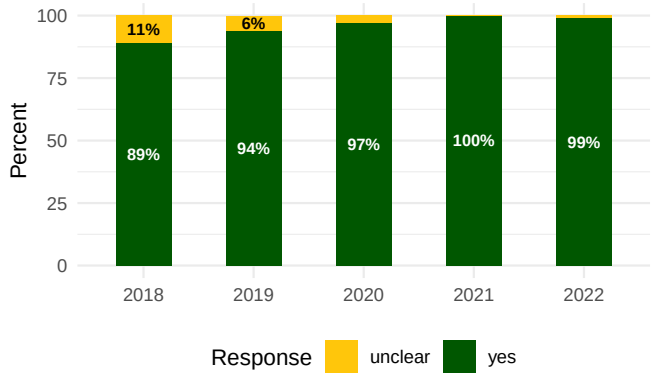
Transparency (What is the Privacy Practice?)

Policy Version

1.1.1: Effective Date

Do the policies clearly indicate the version or effective date of the policies?

Figure 1: Effective Date



The Effective Date evaluation question indicates whether the current version or effective date of the policies is clearly disclosed. The effective date is important to disclose because it provides notice to users if, and when, the terms of a product changed. If a policy's effective date changes, that could also mean that the data collection practices of the product may also have changed and could impact a user's privacy.

Transparent Practice

Privacy policies do indicate a version or effective date.

Statutes & Regulations:

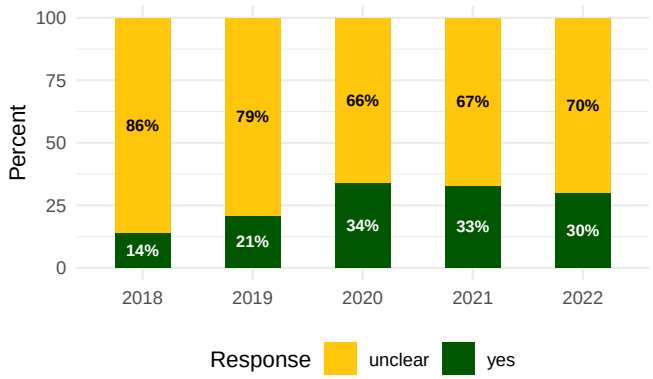
- CalOPPA: (An operator is required to provide notice of the effective or revision date of its privacy policy.)[6]

[6] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(4).

1.1.2: Change Log

Do the policies clearly indicate a changelog or past policy versions are publicly available for review?

Figure 2: Change Log



The Change Log evaluation question indicates whether a public archive or summary of the recent policy changes is available for review. Often it is not clear to a user what additions or deletions were actually made to a policy when the version or effective date changes. Rather than asking users to reread the entire policy and compare the differences between versions, it is better to summarize or indicate what practices changed since the last version that may impact the user's privacy; users can then make a better informed decision whether to continue using the product.

Transparent Practice

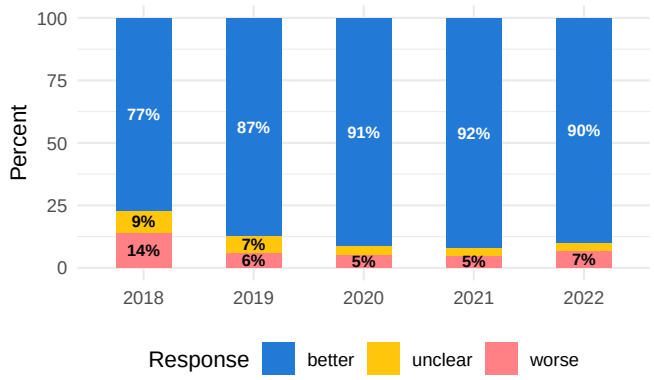
Privacy policies indicate a change log or past policy version is available.

Policy Notice

1.2.1: Change Notice

Do the policies clearly indicate whether or not a user is notified if there are any material changes to the policies?

Figure 3: Change Notice



The Change Notice evaluation question indicates whether or not notification will be provided to users about any changes made to the policies that result in a new version or new effective date of the policies. A company should provide notice to users when they change their policies because the changes may impact the collection or use of a user's data and may change their decision whether to continue using the product.

Better Practice

Users are notified if there are any material changes to the policies.

Worse Practice

Users are not notified if there are any material changes to the policies.

Statutes & Regulations:

- CalOPPA: (An operator is required to describe the process by which they notify consumers who use or visit its website or online service of any material changes to its privacy policy.) [7]
- DSA: (Providers of intermediary services shall inform the recipients of the service of any significant change to the terms and conditions.) [8]

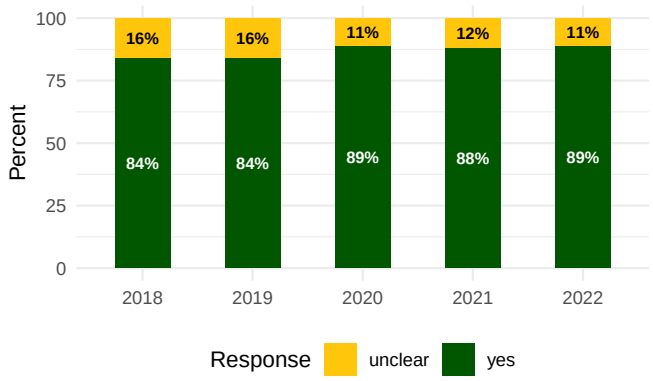
[7] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(3).

[8] Digital Services Act (Regulation (EU) 2022/2065), Terms and conditions, Art. 14(2).

1.2.2: Method Notice

Do the policies clearly indicate the method used to notify a user when policies are updated or materially changed?

Figure 4: Method Notice



The Method Notice evaluation question indicates how users will be directly notified of changes to the company's policy. A company is required to describe the process by which they notify users of changes to policies and obtain consent, which need to be more prominent than simply changing the version or effective date of the policies. Companies need to describe whether they provide adequate notice to users through email, postal mail, mobile notifications, or prominent banners on the website login page or upon launch of a mobile application.

Transparent Practice

Privacy policies indicate the method used to notify a user when policies are updated.

Statutes & Regulations:

- CalOPPA: (An operator is required to describe the process by which they notify consumers who use or visit its website or online service of any material changes to its privacy policy.) [9]

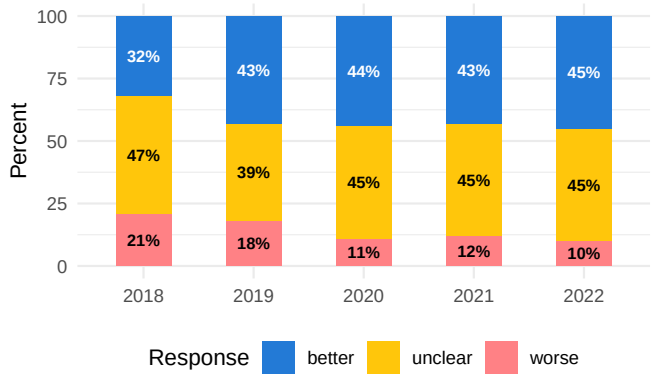
[9] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(3).

Policy Changes

1.3.1: Review Changes

Do the policies clearly indicate whether or not any updates or material changes to the policies will be accessible for review by a user prior to the new changes being effective?

Figure 5: Review Changes



The Review Changes evaluation question indicates the time frame for notification prior to changes to the policies coming into effect. A company should provide adequate time for a user to review any changes to the policies – such as 30 days – to allow the user to make a better informed decision whether to continue using the product.

Better Practice

Users are notified prior to any material changes to the policies.

Worse Practice

Users are not notified prior to any material changes to the policies.

Statutes & Regulations:

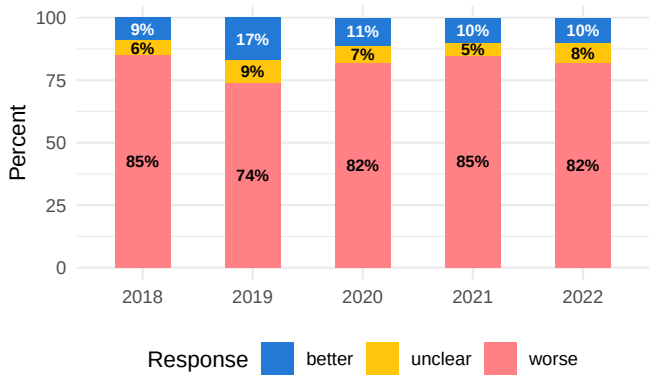
- CalOPPA: (An operator is required to describe the process by which they notify consumers who use or visit its website or online service of any material changes to its privacy policy.) [10]

[10] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(3).

1.3.2: Effective Changes

Do the policies clearly indicate whether or not any changes to the policies are effective immediately and continued use of the product indicates consent?

Figure 6: Effective Changes



The Effective Changes evaluation question indicates whether or not changes to a company's policies are effective immediately without prior review, and whether use of the service by the user indicates consent to any changes. A company should not make changes to its policies that impact the collection or use of a user's personal information without clear notice and informed consent from a user.

Better Practice

Changes to the policies are not effective immediately and continued use of the product requires additional consent.

Worse Practice

Changes to the policies are effective immediately and continued use of the product indicates consent.

Statutes & Regulations:

- CalOPPA: (An operator is required to describe the process by which they notify consumers who use or visit its website or online service of any material changes to its privacy policy.) [11]
- CCPA: (A business may not make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act.) [12]

[11] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(3).

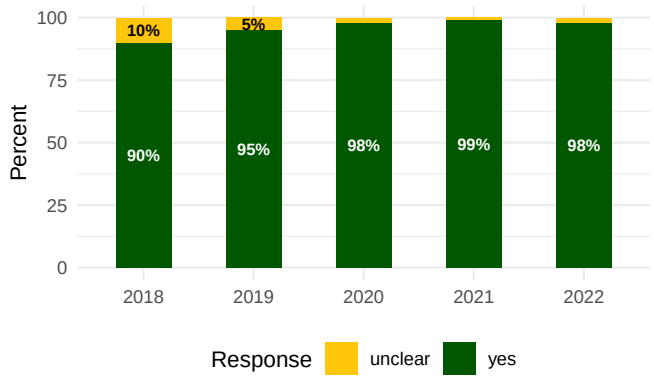
[12] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ad)(2)(C).

Policy Coverage

1.4.1: Services Include

Do the policies clearly indicate which products are covered by the policies?

Figure 7: Services Include



The Services Include evaluation question indicates which websites, apps, or services make up the scope of the company's policies. A company should clearly define what products are covered under the policies so users have clear notice what data collection and use practices apply to which products they use.

Transparent Practice

Privacy policies indicate the products that are covered by the policies.

Statutes & Regulations:

- CalOPPA: (An operator of an online service or application that collects personally identifiable information through the Internet about individual consumers from California who use or visit its service is required to conspicuously post a privacy policy.) [13]

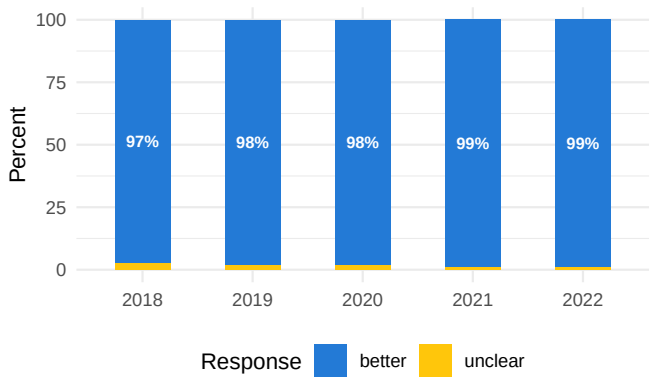
[13] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(a).

Privacy Contact

1.5.1: Company Contact

Do the policies clearly indicate whether or not a user can contact the company about any privacy policy questions, complaints, and changes to the policies?

Figure 8: Company Contact



The Company Contact evaluation question indicates whether privacy contact information of the company is provided for users to ask questions and receive answers about the company's privacy practices or exercise their privacy rights by email, phone number, postal mail, or webform submission.

Better Practice

Users can contact the company about any privacy policy questions, complaints, or material changes to the policies.

Worse Practice

Users cannot contact the company about any privacy policy questions, complaints, or material changes to the policies.

Statutes & Regulations:

- COPPA: (An operator who collects or maintains personal information of children through its website is required to provide contact information in its policies.) [14]
- CalOPPA: (An operator will be in violation if they fail to post or update its policy within 30 days after being notified of noncompliance.) [15]
- CalECA: (The provider of an electronic commercial service must disclose the procedures a consumer may follow in order to resolve a complaint regarding the service or to receive further information regarding use of the service, including the telephone number and address of the Complaint Assistance Unit of the Division of Consumer Services of the Department of Consumer Affairs.) [16]
- GDPR: (Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative.) [17]
- GDPR: (Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: (a) the identity and the contact details of the controller and, if any, of the controller's representative.) [18]
- DSA: (Providers of intermediary services which do not have an establishment in the Union but which offer services in the Union shall designate, in writing, a legal or natural person to act as their legal representative in one of the Member States where the provider offers its services.) [19]

[14] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d)(1).

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

[16] *See* California Electronic Commerce Act, Cal. Civ. Code § 1789.3.

[17] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(1)(a).

[18] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(1)(a).

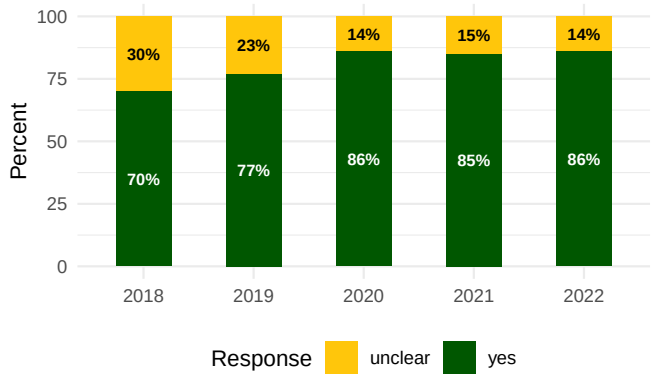
[19] Digital Services Act (Regulation (EU) 2022/2065), Legal representatives, Art. 13.

Policy Principles

1.6.1: Privacy Summary

Do the policies clearly indicate the company's privacy principles by short explanations, layered notices, bullet points, a table of contents, or outlined privacy principles of the company?

Figure 9: Privacy Summary



The Privacy Summary evaluation question indicates whether a company's privacy principles, easy-to-read summary, table of contents, or explanations of the practices of the privacy policy are disclosed. A company should provide clear notice of the most important privacy practices to help users clearly understand the privacy concerns that matter most to them and to make a better informed decision whether to use the product.

Transparent Practice

Privacy policies do indicate privacy principles, layered notices, or a table of contents.

Statutes & Regulations:

- GDPR: (This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.) [20]
- GDPR: (The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.) [21]
- GDPR: (Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.) [22]
- GDPR: (The controller shall take appropriate measures to provide any information ... relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.) [23]

[20] *See* General Data Protection Regulation (GDPR) 2016/679, Subject-matter and objectives, Art. 1(2).

[21] *See* General Data Protection Regulation (GDPR) 2016/679, Subject-matter and objectives, Art. 1(3).

[22] *See* General Data Protection Regulation (GDPR) 2016/679, Principles relating to processing personal data, Art. 5(1)(a).

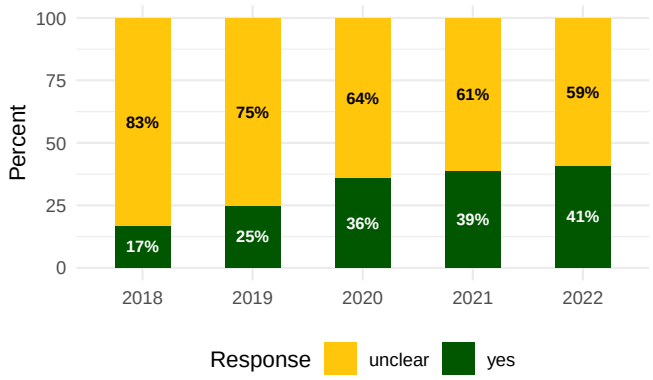
[23] General Data Protection Regulation (GDPR) 2016/679, Transparent information communication and modalities for the exercise of the rights of the data subject, Art. 12(1).

Policy Language

1.7.1: Preferred Language

Do the policies clearly indicate they are available in any language(s) other than English?

Figure 10: Preferred Language



The Preferred Language evaluation question indicates whether the policies are available in other languages, or, more importantly, the language most commonly spoken by the user. A company with users in more than one country should provide its policies in all of the languages spoken by its users to ensure adequate notice and informed consent is given by each user to the company's privacy practices.

Transparent Practice

Privacy policies are available in multiple languages.

Statutes & Regulations:

- DSA: (Very large online platforms and very large online search engines shall publish their terms and conditions in the official languages of all the Member States in which they offer their services.) [24]
- GDPR: (The controller shall take appropriate measures to provide any information ... relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.) [25]

[24] Digital Services Act (Regulation (EU) 2022/2065), Terms and conditions, Art. 14(6).

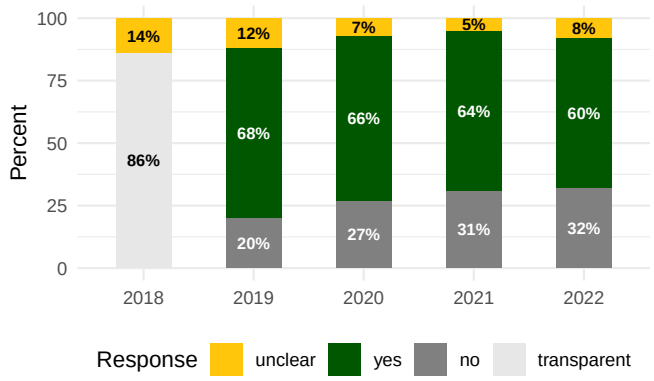
[25] *See* General Data Protection Regulation (GDPR) 2016/679, Transparent information communication and modalities for the exercise of the rights of the data subject, Art. 12(1).

Intended Use

1.8.1: Children Intended

Do the policies clearly indicate whether or not the product is intended to be used by children under the age of 13?

Figure 11: Children Intended



The Children Intended evaluation question indicates whether children under 13 years of age are intended users of the product. A company should disclose all the intended audiences of their product because different privacy laws and protections apply to different users, especially children.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

- COPPA: (A site directed to children is where the operator has actual knowledge the site is collecting information from children under the age of 13 and parental consent is required before any collection or use of information.) [26]
- GDPR: (In relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.) [27]
- CAADCA: (Children should be afforded protections not only by online products and services directed at them but by all online products and services they are likely to access. Businesses that develop and provide online services, products, or features that children are likely to access should consider the best interests of children when designing, developing, and providing that online service, product, or feature.) [28]
- CAADCA: (A "child" or "children" means consumers who are under 18 years of age.) [29]
- CAADCA: (A product or service "likely to be accessed by children" means it is reasonable to expect, based on specified indicators, that the online service, product, or feature would be accessed by children.) [30]
- CAADCA: (A business shall estimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data practices of the business, or apply the privacy and data protections afforded to children to all consumers.) [31]
- DSA: (Where an intermediary service is primarily directed at minors or is predominantly used by them, the provider of that intermediary service shall explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand.) [32]

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

[27] General Data Protection Regulation (GDPR) 2016/679, Conditions Applicable to Child's Consent in Relation to Information Society Services, Art. 8(1).

[28] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.29(a).

[29] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.30(b)(1).

[30] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.30(b)(4)(A),(B), (D)-(F).

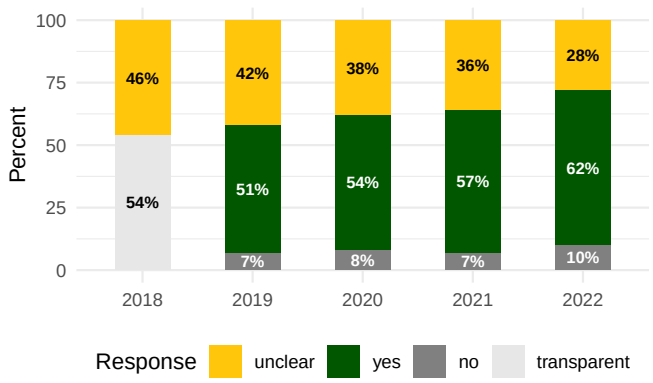
[31] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(a)(5).

[32] Digital Services Act (Regulation (EU) 2022/2065), Terms and conditions, Art. 14(2).

1.8.2: Teens Intended

Do the policies clearly indicate whether or not the product is intended to be used by teens 13 to 18 years of age?

Figure 12: Teens Intended



The Teens Intended evaluation question indicates whether teens over 13 years of age, but under 18 years of age, are intended users of the product. A company should disclose all the intended audiences of their product because different privacy laws and protections apply to different users, including teens under the age of majority in their respective country.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

- COPPA: (A mixed audience site is where the site is directed to children, but does not target children as its "primary audience," but rather teens 13-to-18 years of age or adults. An operator of a mixed audience site is required to obtain age information from a user before collecting any information and if a user identifies themselves as a child under the age of 13, the operator must obtain parental consent before any information is collected.) [33]
- CalPRMDW: (Prohibits an operator from marketing or advertising non age-appropriate types of products or services to a minor under 18 years of age and from knowingly using, disclosing, compiling, or allowing a third party to use, disclose, or compile, the personal information of a minor for the purpose of marketing or advertising non age-appropriate types of products or services. Also, a minor is permitted to request to "erase" or remove and obtain removal of content or information posted on the operator's site.) [34]
- GDPR: (In relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.) [35]
- CAADCA: (A "child" or "children" means consumers who are under 18 years of age.) [36]

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

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

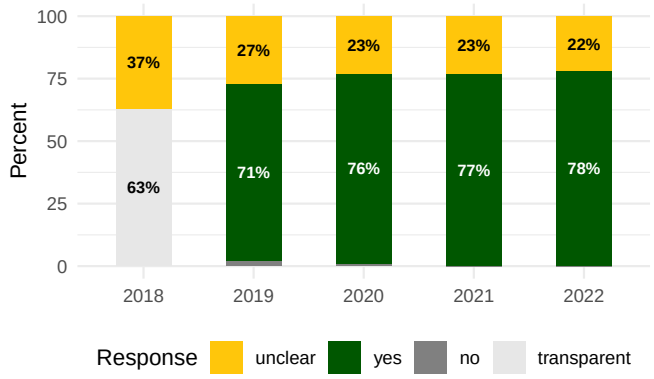
[35] General Data Protection Regulation (GDPR) 2016/679, Conditions Applicable to Child's Consent in Relation to Information Society Services, Art. 8(1).

[36] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.30(b)(1).

1.8.3: Adults Intended

Do the policies clearly indicate whether or not the product is intended to be used by adults over the age of 18?

Figure 13: Adults Intended



The Adults Intended evaluation question indicates whether individuals over the age of majority in their respective country are intended users of the product. A company should disclose all the intended audiences of their product because different privacy laws and protections apply to different users.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

- COPPA: (A general audience site is where the operator has no actual knowledge that a child under the age of 13 has registered an account or is using the service, and no age gate or parental consent is required before collection of information.) [37]
- GDPR: (This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.) [38]
- CCPA: (Consumer' means a natural person who is a California resident however identified, including by any unique identifier.) [39]

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

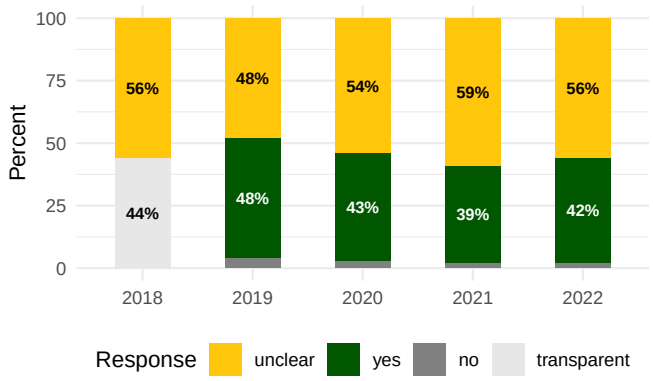
[38] General Data Protection Regulation (GDPR) 2016/679, Subject-matter and objectives, Art. 1(1).

[39] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(i).

1.8.4: Parents Intended

Do the policies clearly indicate whether or not the product is intended to be used by parents or guardians?

Figure 14: Parents Intended



The Parents Intended evaluation question indicates whether individuals with children who are users of the product are also intended users of the product. A company should disclose all the intended audiences of their product because different privacy laws and protections apply to different users which include the ability of parent users to manage child profiles and provide consent on behalf of their children.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

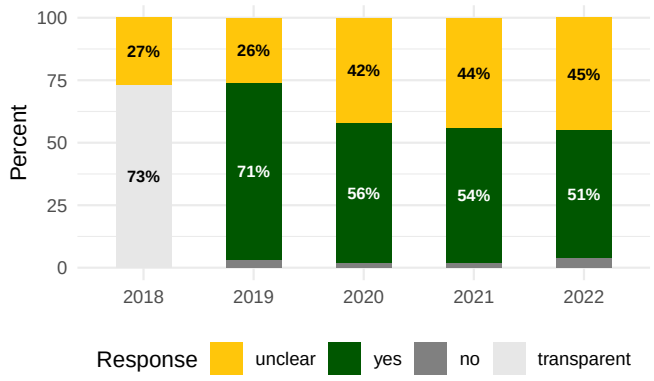
- COPPA: (An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology and existing methods available to a parent to prove their identity.) [40]

[40] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(b)(i)-(iv).

1.8.5: Students Intended

Do the policies clearly indicate whether or not the product is intended to be used by students in preschool or preK-12?

Figure 15: Students Intended



The Students Intended evaluation question indicates whether children under 13 years of age and teens over 13 years of age, but under 18 years of age, are the intended audience of the product for use in a preschool or preK-12 school or district. A company should disclose all the intended audiences of their product because different privacy laws and protections apply to different users, including students with additional federal and state student data privacy laws.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

- SOPIPA: (SOPIPA applies to operators of online services that are primarily used for K-12 school purposes and were designed and marketed for K-12 school purposes.)[41]
- ELPIPA: (ELPIPA applies to operators of online services that are primarily used for preschool or prekindergarten purposes and were designed and marketed for preschool or prekindergarten purposes.)[42]
- SOPIPA: (SOPIPA does not apply to general audience websites and services that are not primarily used by K-12 students.)[43]
- FERPA: ("Personal Information" under FERPA includes direct identifiers such as a student or family member's name, or indirect identifiers such as a date of birth, or mother's maiden name, or other information that is linkable to a specific student that would allow a reasonable person in the school community to identify the student with reasonable certainty.)[44]
- CalPPR: (Prohibits schools, school districts, county offices of education, and charter schools from collecting or maintaining information about pupils from social media for any purpose other than school or pupil safety, without notifying each parent or guardian and providing the pupil with access and an opportunity to correct or delete such information.)[45]

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

[42] Early Learning Personal Information Protection Act (ELPIPA), Cal. B.&P. Code § 22586(a)(1).

[43] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(m).

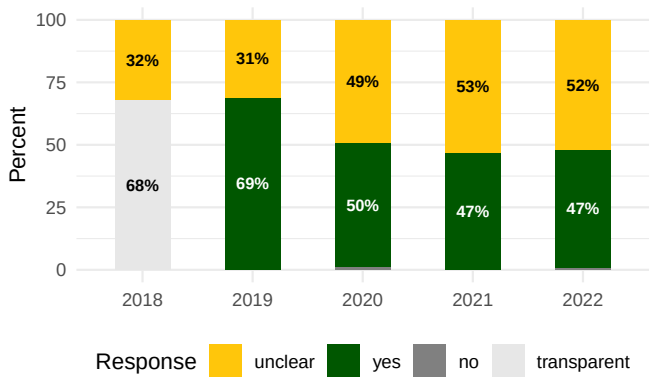
[44] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.

[45] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.6(c).

1.8.6: Teachers Intended

Do the policies clearly indicate whether or not the product is intended to be used by teachers?

Figure 16: Teachers Intended



The Teachers Intended evaluation question indicates whether individuals in a K-12 school or district with students who are users of the product are also intended users of the product. A company should disclose all the intended audiences of their product because different privacy laws and protections apply to different users, which include the ability of teacher users to manage student accounts and provide consent on behalf of their parents.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

- FERPA: (FERPA applies to all educational institutions that accept public funds under a program of the U.S. Department of Education.)[46]
- SOPIPA: (SOPIPA applies to operators of online services that are primarily used for K-12 school purposes and were designed and marketed for K-12 school purposes.)[47]
- ELPIPA: (ELPIPA applies to operators of online services that are primarily used for preschool or prekindergarten purposes and were designed and marketed for preschool or prekindergarten purposes.)[48]
- PPRA: (All instructional materials including teacher's manuals, films, tapes, or other supplementary instructional material which is used in connection with any research must be made available for inspection by the parents or guardians of the children.)[49]
- FERPA: (An exception for disclosing personally identifiable information without obtaining parental consent exists for sharing with other school officials, including teachers within the same educational institution.)[50]
- SOPIPA: ("Covered Information" under SOPIPA is personally identifiable information that includes descriptive information or identifies a student that was created or provided by a student, parent, teacher, district staff, or gathered by an operator through the operation of the site.)[51]

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

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

[48] *See* Early Learning Personal Information Protection Act (ELPIPA), Cal. B.&P. Code § 22586(a)(1).

[49] Protection of Pupil Rights Act (PPRA), 34 C.F.R. §98.3.

[50] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(i)(A).

[51] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(i)(1)-(3).

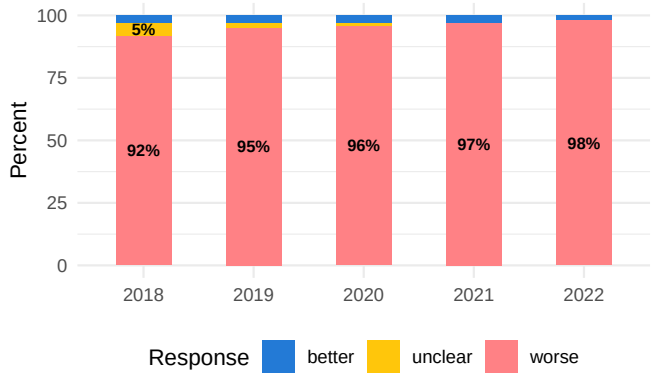
Focused Collection (What Information is Collected?)

Data Collection

2.1.1: Collect PII

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

Figure 17: Collect PII



The Collect Personally Identifiable Information evaluation question indicates whether or not personal information is collected by the product. A company should disclose whether the product collects personal information from any user, because the collection of personal information can increase risk depending on the amount of personal information collected and how it is used.

Better Practice

Personally identifiable information (PII) is not collected.

Worse Practice

Personally identifiable information (PII) is collected.

Statutes & Regulations:

- COPPA: (Personally Identifiable Information under COPPA includes first and last name, photos, videos, audio, geolocation information, persistent identifiers, IP address, cookies, and unique device identifiers.) [52]
- CalOPPA: (The term "Personally Identifiable Information" under CalOPPA means individually identifiable information about a consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following: (1) A first and last name; (2) A home or other physical address, including street name and name of a city or town; (3) An e-mail address; (4) A telephone number; (5) A social security number; or (6) Any other identifier that permits the physical or online contacting of a specific individual.) [53]
- FERPA: ("Personal Information" under FERPA includes direct identifiers such as a student or family member's name, or indirect identifiers such as a date of birth, or mother's maiden name, or other information that is linkable to a specific student that would allow a reasonable person in the school community to identify the student with reasonable certainty.) [54]
- GDPR: ("Personal data" means any information relating to an identified or identifiable natural person ("data subject") such as an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.) [55]
- CCPA: (A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the specific pieces of personal information it has collected about that consumer.) [56]
- CCPA: ("Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.) [57]
- CCPA: ("Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.) [58]

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

[53] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22577(a)(1)-(6).

[54] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.

[55] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(1).

[56] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.110(a)(5).

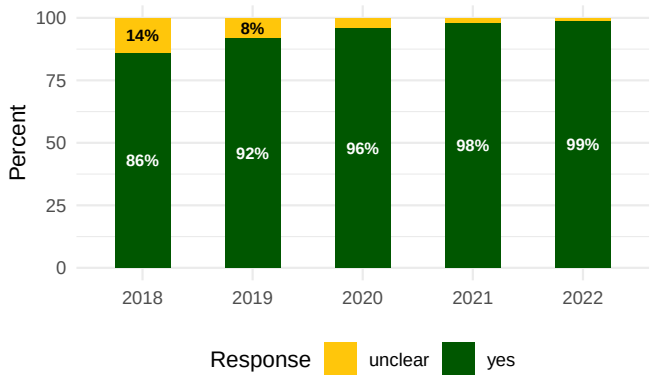
[57] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(f).

[58] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(v)(1).

2.1.2: PII Categories

Do the policies clearly indicate what type of categories of personally identifiable information are collected?

Figure 18: PII Categories



The Personally Identifiable Information Categories evaluation question indicates what categories of personal information are collected by the product. A company should disclose what categories of personal information the product collects from any user, because the collection of personal information can increase risk depending on what types of personal information are collected and how it is used.

Transparent Practice

The categories of collected personally identifiable information are indicated.

Statutes & Regulations:

- CalOPPA: (An operator is required to identify the categories of personally identifiable information that they collect about individual consumers who use or visit its website or online service.) [59]
- COPPA: (A parent or guardian can request the operator to provide a description of the specific types or categories of personal information collected from children by the application or service.) [60]
- GDPR: (Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: ... (d) the categories of personal data concerned.) [61]
- GDPR: (The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: ... (b) the categories of personal data concerned.) [62]
- CCPA: (A business that controls the collection of a consumer's personal information shall inform consumers as to categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether such information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, without providing the consumer with notice consistent with this section.) [63]
- CCPA: (A consumer shall have the right to request that a business that collects personal information about the consumer disclose the categories of personal information it has collected about that consumer.) [64]
- CCPA: (A consumer shall have the right to request that a business that sells or shares the consumer's personal information disclose to that consumer the categories of personal information that the business collected about the consumer.) [65]
- CCPA: (A business shall disclose in its online privacy policy a list of the categories of personal information it has collected about consumers in the preceding 12 months.) [66]
- CCPA: (Personal Information includes any personal information described as "customer records.".) [67]
- CCPA: ("Probabilistic identifier" means the identification of a consumer or a consumer's device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.) [68]
- Telecom Act: (The term "subscriber list information" means any information identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications, or any combination of such listed names, numbers, addresses, or classifications.) [69]

[59] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(1).

[60] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.6(a)(1).

[61] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(1)(d).

[62] General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(1)(b).

[63] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100(a)(1).

[64] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.110(a)(1).

[65] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.115(a)(1).

[66] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.130(a)(5)(B)(i).

[67] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(v)(1)(B).

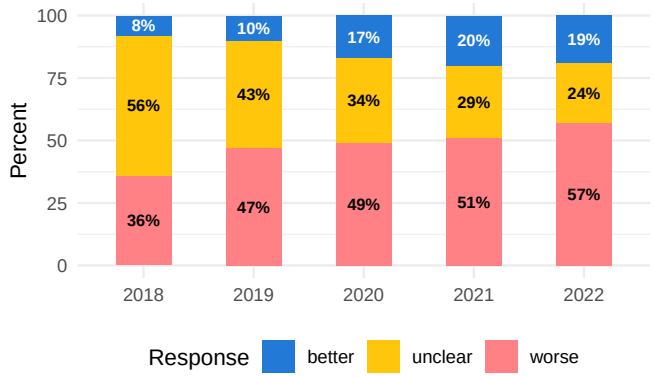
[68] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(x).

[69] *See* Telecommunications Act, Privacy of customer information, 47 U.S. Code § 222(h)(3)(A).

2.1.3: Geolocation Data

Do the policies clearly indicate whether or not geolocation data are collected?

Figure 19: Geolocation Data



The Geolocation Data evaluation question indicates whether or not location information is collected from the product or derived from usage information including GPS, IP address, or other methods. A company should disclose whether location information is collected and how that information is collected because there is an increased risk if a user's location is known in real time or can be tracked over time.

Better Practice

Geolocation data are not collected.

Worse Practice

Geolocation data are collected.

Statutes & Regulations:

- COPPA: (Personally Identifiable Information under COPPA includes first and last name, photos, videos, audio, geolocation information, persistent identifiers, IP address, cookies, and unique device identifiers.) [70]
- FERPA: ("Personal Information" under FERPA includes direct identifiers such as a student or family member's name, or indirect identifiers such as a date of birth, or mother's maiden name, or other information that is linkable to a specific student that would allow a reasonable person in the school community to identify the student with reasonable certainty.) [71]
- SOPIPA: ("Covered Information" under SOPIPA is personally identifiable information that includes descriptive information or identifies a student that was created or provided by a student, parent, teacher, district staff, or gathered by an operator through the operation of the site.) [72]
- CalOPPA: (The term "Personally Identifiable Information" under CalOPPA means individually identifiable information about a consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following: ... (6) Any other identifier that permits the physical or online contacting of a specific individual.) [73]
- GDPR: ("Personal data" means any information relating to an identified or identifiable natural person ("data subject") such as an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.) [74]
- CCPA: ("Precise geolocation" means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of one thousand, eight hundred and fifty (1,850) feet, except as prescribed by regulations.) [75]
- CAADCA: (A business shall not collect, sell, or share any precise geolocation information of children by default unless the collection of that precise geolocation information is strictly necessary for the business to provide the service, product, or feature requested. The business is also required to provide an obvious sign to the child that precise geolocation information is being collected.) [76]
- Telecom Act: (Customer call location information concerning the user of a commercial mobile service or the user of an IP-enabled voice service shall not be disclosed to a third-party without express prior authorization of the customer.) [77]

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

[71] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.

[72] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(i)(1)-(3).

[73] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22577(a)(6).

[74] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(1).

[75] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(w).

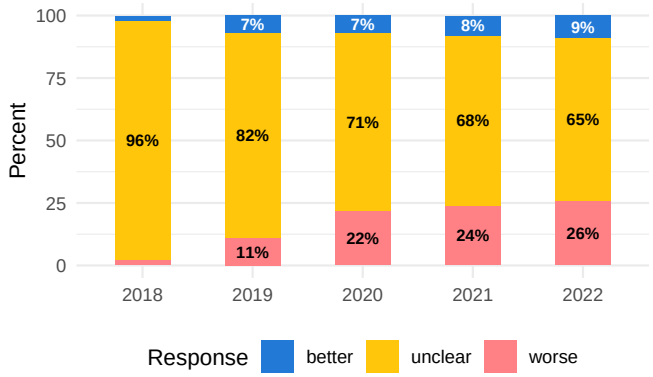
[76] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(b)(5),(6).

[77] *See* Telecommunications Act, Privacy of customer information, 47 U.S. Code § 222(f)(1).

2.1.4: Health Data

Do the policies clearly indicate whether or not any health or biometric data are collected?

Figure 20: Health Data



The Health Data evaluation question indicates whether or not health or biometric data is collected by the product. This may include body movements, heart rate, fingerprint, iris scan, or other biological activity related to a specific individual. A company should disclose whether health or biometric information is collected and how that information is collected, because there is an increased risk if a user's health information is used for unintended purposes.

Better Practice

Biometric or health data are not collected.

Worse Practice

Biometric or health data are collected.

Statutes & Regulations:

- FERPA: (A biometric record, as used in the definition of personally identifiable information, means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.)[78]
- COPPA: (Personally Identifiable Information under COPPA includes first and last name, photos, videos, audio, geolocation information, persistent identifiers, IP address, cookies, and unique device identifiers.)[79]
- SOPIPA: ("Covered Information" under SOPIPA is personally identifiable information that includes descriptive information or identifies a student that was created or provided by a student, parent, teacher, district staff, or gathered by an operator through the operation of the site.)[80]
- GDPR: ("Personal data" means any information relating to an identified or identifiable natural person ("data subject") such as an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.)[81]
- GDPR: ("Genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.)[82]
- GDPR: ("Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.)[83]
- GDPR: ("data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.)[84]
- CCPA: ("Biometric information" means an individual's physiological, biological or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or intended to be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.)[85]

[78] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.

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

[80] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(i)(1)-(3).

[81] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(1).

[82] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(13).

[83] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(14).

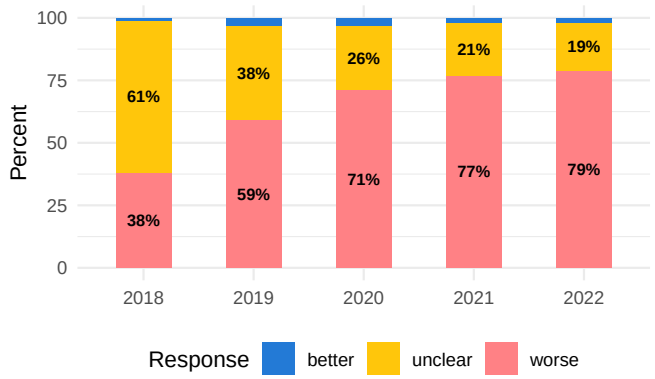
[84] >General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(15).

[85] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(c).

2.1.5: Behavioral Data

Do the policies clearly indicate whether or not any behavioral or activity related data are collected?

Figure 21: Behavioral Data



The Behavioral Data evaluation question indicates whether or not a user's interactions, behaviors, or usage analytics with the product are collected. For example, behavioral data can include which features are used or not used, which buttons or controls are clicked, and which content is viewed, what other users viewed that same content and when, and the duration of interactions with the product and other users – all of which can all be used to create a behavioral profile of the user. The collection of behavioral data can reveal significant information about a user's preferences, habits, and vulnerabilities that can increase risk if used for unintended purposes.

Better Practice

Interactions, behaviors, or usage analytics data are not collected.

Worse Practice

Interactions, behaviors, or usage analytics data are collected.

Statutes & Regulations:

- COPPA: (An operator is prohibited from including behavioral advertisements or amassing a profile of a child under the age of 13 child without parental consent.) [86]
- FERPA: (A biometric record, as used in the definition of personally identifiable information, means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.) [87]
- GDPR: ("Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.) [88]
- CCPA: ("Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.) [89]
- CCPA: ("Intentionally interacts" means when the consumer intends to interact with a person, or disclose personal information to a person, via one or more deliberate interactions, such as visiting the person's website or purchasing a good or service from the person. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a person.) [90]
- CAADCA: (A business shall not profile a child by default unless the business can demonstrate it has appropriate safeguards in place to protect children, and profiling is necessary to provide the online service, product, or feature requested, or the business can demonstrate a compelling reason that profiling is in the best interests of children.) [91]
- CCPA: ("Personal information" includes inferences drawn from any information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.) [92]

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

[87] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.

[88] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(14).

[89] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(r).

[90] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(s).

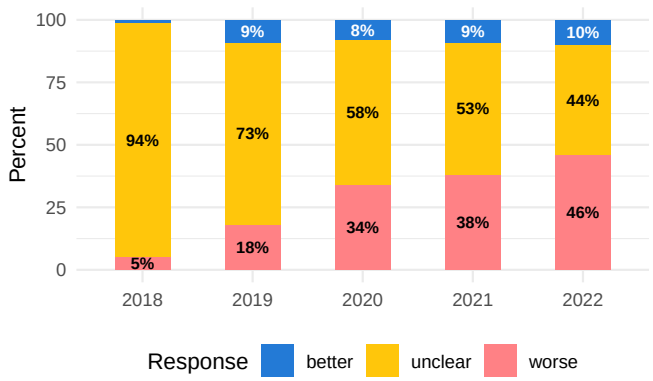
[91] *See* California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(b)(2)(A)-(B).

[92] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(v)(1)(K).

2.1.6: Sensitive Data

Do the policies clearly indicate whether or not sensitive personal information is collected?

Figure 22: Sensitive Data



The Sensitive Data evaluation question indicates whether or not specific information protected under federal or state law is collected by the product. For example, sensitive data can include race, ethnicity, gender, sexual identity, religion, political affiliation, national origin, and financial information. The collection of sensitive data can reveal significant information about a user that can increase risk if used for discriminatory or other unintended purposes.

Better Practice

Sensitive data are not collected.

Worse Practice

Sensitive data are collected.

Statutes & Regulations:

- GDPR: (Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited unless: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition ... may not be lifted by the data subject.) [93]
- CCPA: (A business that controls the collection of a consumer's personal information shall inform consumers if the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used and whether such information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected, without providing the consumer with notice consistent with this section.) [94]
- CCPA: (A consumer shall have the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services.) [95]
- CCPA: (A business that has received direction from a consumer not to use or disclose the consumer's sensitive personal information shall be prohibited from using or disclosing the consumer's sensitive personal information for any other purpose after its receipt of the consumer's direction, unless the consumer subsequently provides consent for the use or disclosure of the consumer's sensitive personal information for additional purposes.) [96]
- CCPA: (The term "personal information" includes sensitive personal information.) [97]
- CCPA: ("Sensitive personal information" means personal information that reveals a consumer's social security, driver's license, state identification card, or passport number; or a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; or a consumer's precise geolocation; or a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; or the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication; or a consumer's genetic data.) [98]

[93] General Data Protection Regulation (GDPR) 2016/679, Processing of special categories of personal data, Art. 9(1)-(2)(a).

[94] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100(a)(2).

[95] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.121(a).

[96] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.121(b).

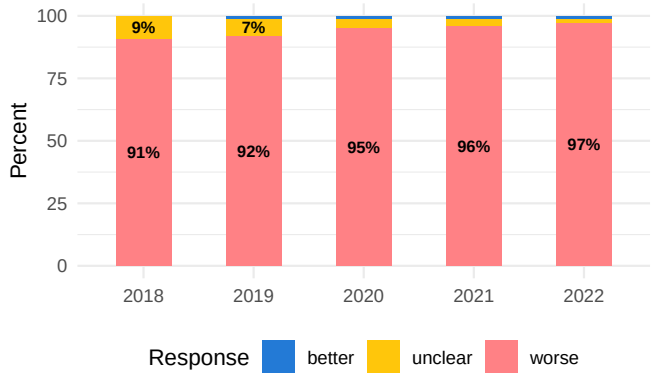
[97] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(v)(1)(L).

[98] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ae)(1).

2.1.7: Usage Data

Do the policies clearly indicate whether or not any data is collected automatically?

Figure 23: Usage Data



The Usage Data evaluation question indicates whether or not a user's device information or technical analytics with the product are collected. For example, usage data can include a user's IP address, device unique identifier, advertising identifier, persistent cookies, time stamps, amount of data downloaded or uploaded, filenames, network IDs, or other identifiers. The collection of usage data can reveal significant information about a user's devices used to access the product and identity that can increase risk if used for unintended purposes.

Better Practice

Data is not automatically collected.

Worse Practice

Data is automatically collected.

Statutes & Regulations:

- COPPA: (Personally Identifiable Information under COPPA includes first and last name, photos, videos, audio, geolocation information, persistent identifiers, IP address, cookies, and unique device identifiers.) [99]
- FERPA: ("Personal Information" under FERPA includes direct identifiers such as a student or family member's name, or indirect identifiers such as a date of birth, or mother's maiden name, or other information that is linkable to a specific student that would allow a reasonable person in the school community to identify the student with reasonable certainty.) [100]
- SOPIPA: ("Covered Information" under SOPIPA is personally identifiable information that includes descriptive information or identifies a student that was created or provided by a student, parent, teacher, district staff, or gathered by an operator through the operation of the site.) [101]
- CalOPPA: (The term "Personally Identifiable Information" under CalOPPA means individually identifiable information about a consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following: ... (6) Any other identifier that permits the physical or online contacting of a specific individual.) [102]
- GDPR: ("Personal data" means any information relating to an identified or identifiable natural person ("data subject") such as an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.) [103]
- CCPA: (The term "personal information" includes Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.) [104]
- Telecom Act: (The term "customer proprietary network information (CPNI)" means information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship.) [105]

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

[100] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.

[101] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(i)(1)-(3).

[102] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22577(a)(6).

[103] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(1).

[104] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(v)(1)(F).

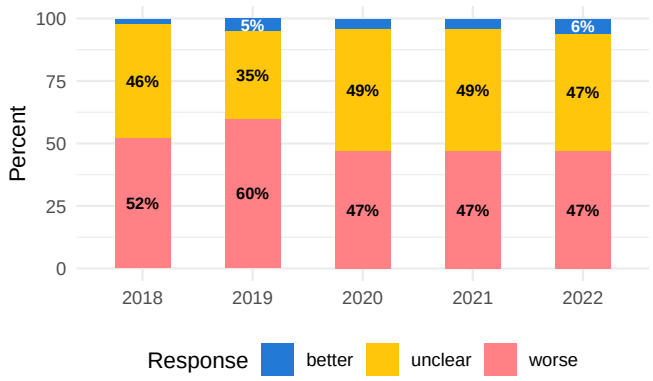
[105] Telecommunications Act, Privacy of customer information, 47 U.S. Code § 222(h)(1)(A).

Data Source

2.2.1: Student Data

Do the policies clearly indicate whether or not the company collects personal information or education records from preK-12 students?

Figure 24: Student Data



The Student Data evaluation question indicates whether information related to a student's use of the product in a K-12 school or district is collected for education purposes. A company should disclose whether student data is collected from any user of the product because of the additional student data privacy protections required for collection and use of education records under federal and state law.

Better Practice

Personal information or education records are not collected from preK-12 students.

Worse Practice

Personal information or education records are collected from preK-12 students.

Statutes & Regulations:

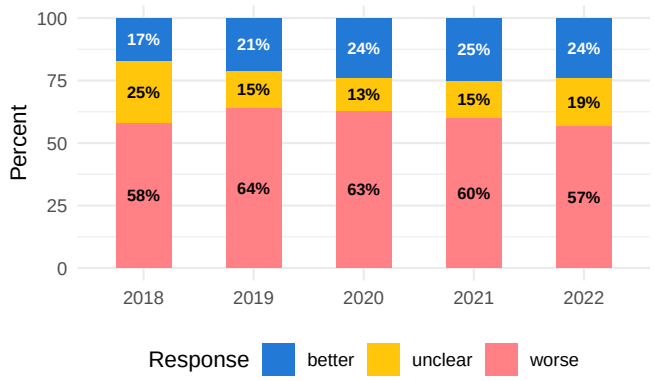
- FERPA: ("Education Records" are information that is directly related to a student and maintained by the educational institution, or by a third party acting as a School Official on behalf of the educational institution.) [106]
- FERPA: ("Personal Information" under FERPA includes direct identifiers such as a student or family member's name, or indirect identifiers such as a date of birth, or mother's maiden name, or other information that is linkable to a specific student that would allow a reasonable person in the school community to identify the student with reasonable certainty.) [107]
- SOPIPA: (SOPIPA applies to operators of online services that are primarily used for K-12 school purposes and were designed and marketed for K-12 school purposes.) [108]
- ELPIPA: (ELPIPA applies to operators of online services that are primarily used for preschool or prekindergarten purposes and were designed and marketed for preschool or prekindergarten purposes.) [109]

[106] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.
[107] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.
[108] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(a).
[109] Early Learning Personal Information Protection Act (ELPIPA), Cal. B.&P. Code § 22586(a)(1).

2.2.2: Child Data

Do the policies clearly indicate whether or not the company collects personal information from children under 13 years of age?

Figure 25: Child Data



The Child Data evaluation question indicates whether information related to a child under 13 years of age is collected by the product. A company should disclose whether child data is collected from any user of the product because of the additional privacy protections required for the collection and use of children's personal information under federal law.

Better Practice

Personal information from children under 13 years of age is not collected.

Worse Practice

Personal information from children under 13 years of age is collected.

Statutes & Regulations:

- COPPA: (A notice or privacy policy on an operator's website needs a section relating to the collection of information for children under 13 years of age, and notice is required at each area of the site where information is collected from children.) [110]
- COPPA: (Personally Identifiable Information under COPPA includes first and last name, photos, videos, audio, geolocation information, persistent identifiers, IP address, cookies, and unique device identifiers.) [111]
- CAADCA: (A business shall not collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, unless the business can demonstrate a compelling reason that the collecting, selling, sharing, or retaining of the personal information is in the best interests of children.) [112]

[110] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d).

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

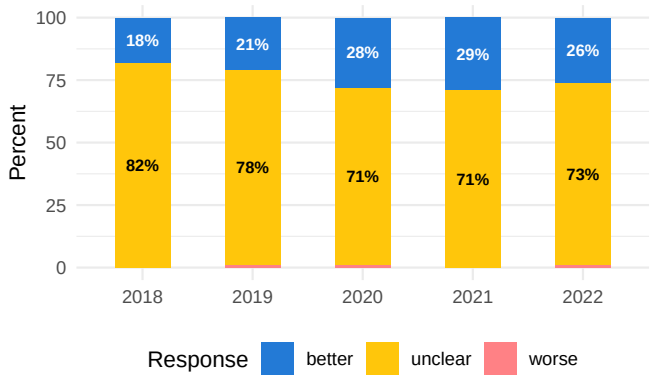
[112] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(b)(3).

Data Excluded

2.3.1: Data Excluded

Do the policies clearly indicate whether or not the company excludes specific types of data from collection?

Figure 26: Data Excluded



The Data Excluded evaluation question indicates whether specific types of personal information are excluded from collection by the product either because of a concern for the sensitive nature of the information, or that a third-party service provider may collect that type of personal information on behalf of the company. A company should minimize the collection of information to only data required to provide the product and exclude collection of unnecessary data.

Better Practice

Specific types of personal information are excluded from collection.

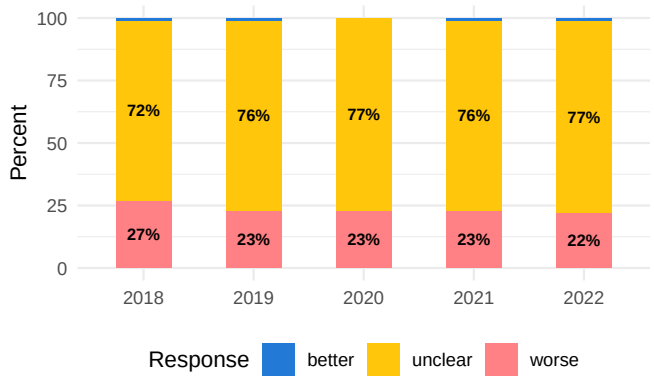
Worse Practice

Specific types of personal information are not excluded from collection.

2.3.2: Coverage Excluded

Do the policies clearly indicate whether or not the company excludes specific types of collected data from coverage under its privacy policy?

Figure 27: Coverage Excluded



The Coverage Excluded evaluation question indicates whether specific types of information that are collected by the product or third parties are excluded from the scope of the privacy policy either because of a concern for the sensitive nature of the information, or that a third-party service provider's policies cover the data collection and use practices for that type of information. A company should not collect information from users that is not covered by the product's privacy policies to ensure users have adequate notice of how their data will be collected and used in order to provide informed consent.

Better Practice

Specific types of collected information are not excluded from the privacy policy.

Worse Practice

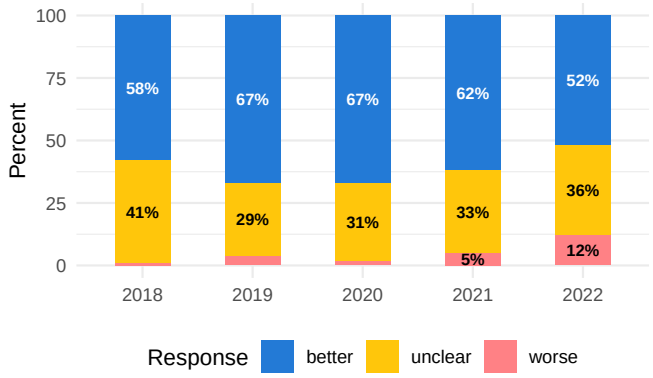
Specific types of collected information are excluded from the privacy policy.

Data Limitation

2.4.1: Collection Limitation

Do the policies clearly indicate whether or not the company limits the collection of information to only data that are specifically required for the product?

Figure 28: Collection Limitation



The Collection Limitation evaluation question indicates whether information is only collected that is necessary for providing the primary purpose of the product. A company should practice data minimization principles and only collect the minimum amount of data required to provide the product to users in order to decrease the risk that a user's data is used for unintended purposes.

Better Practice

Collection or use of data is limited to product requirements.

Worse Practice

Collection or use of data is not limited to product requirements.

Statutes & Regulations:

- COPPA: (A vendor is prohibited from conditioning a child's participation in a game or prize on the child disclosing more info than necessary to participate in the activity.) [113]
- GDPR: (Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.) [114]
- GDPR: (When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.) [115]
- GDPR: (Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.) [116]
- CCPA: (A business's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.) [117]
- CAADCA: (A business shall not use personal information of a child for any reason other than a reason for which that personal information was collected, unless the business can demonstrate a compelling reason that use of the personal information is in the best interests of children.) [118]
- CAADCA: (A business shall not use dark patterns to encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being.) [119]

[113] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.7.

[114] General Data Protection Regulation (GDPR) 2016/679, Principles relating to processing of personal data, Art. 5(1)(c).

[115] General Data Protection Regulation (GDPR) 2016/679, Conditions for Consent, Art. 7(4).

[116] General Data Protection Regulation (GDPR) 2016/679, Data protection by design and by default, Art. 25(1).

[117] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100(c).

[118] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(b)(4).

[119] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(b)(7).

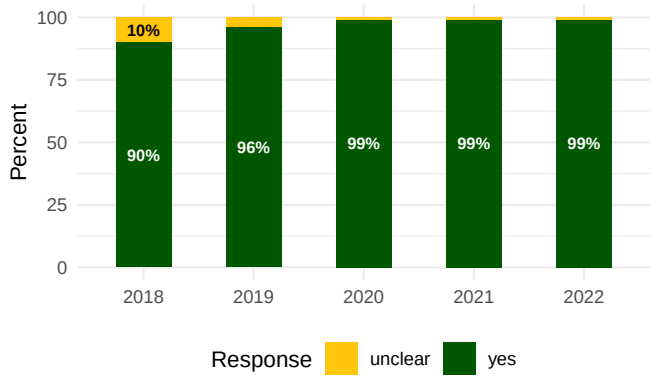
Data Sharing (How do Third-Parties Collect, Access, and Use Data?)

Data Shared With Third Parties

3.1.1: Data Shared

Do the policies clearly indicate if collected information (this includes data collected via automated tracking or usage analytics) is shared with third parties?

Figure 29: Data Shared



The Data Shared evaluation question indicates if the product shares a user's data with third parties. Sharing a user's data with third parties is not qualitatively better or worse because it is often a necessary requirement to provide all the features of a product that includes sharing data with third-party service providers such as SDKs, cloud hosting, content integrations, or payment processors.

Transparent Practice

Collected information is shared with third parties.

Statutes & Regulations:

- COPPA: (Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.) [120]
- COPPA: (An operator may share data with third parties who provide support for the "internal operations" of the service and who do not use or disclose the information for any other purpose.) [121]
- COPPA: (An operator must take reasonable steps to release a child's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of the information, and provide assurances that they contractually maintain the information in the same manner.) [122]
- COPPA: (An operator can not condition a child's participation in the service by sharing any collected information with third parties. A parent is required to have the ability to consent to the collection and use of their child's personal information without also consenting to the disclosure of the information to third parties.) [123]
- FERPA: (A school is prohibited from disclosing a student's "education record" or data to third parties without parental consent.) [124]
- SOPIPA: (An operator is prohibited from sharing student information to third parties except in limited circumstances to other schools, or for research purposes.) [125]
- GDPR: ("recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.) [126]
- GDPR: ("third party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.) [127]
- CCPA: ("Share," "shared," or "sharing" 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.) [128]

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

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

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

[123] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(a)(2).

[124] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30.

[125] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4).

[126] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(9.)

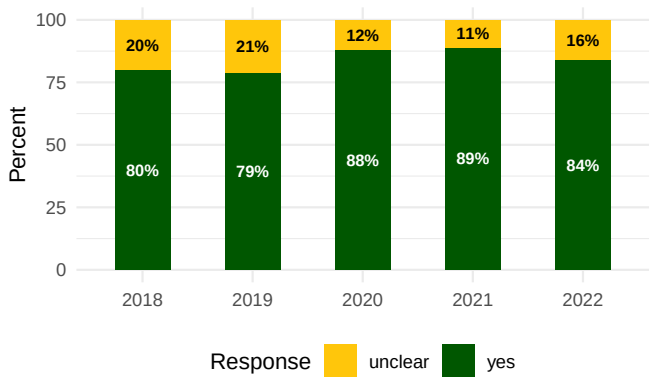
[127] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(10).

[128] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ah).

3.1.2: Data Categories

Do the policies clearly indicate what type of categories of information are shared with third parties?

Figure 30: Data Categories



The Data Categories evaluation question indicates whether the product shares a user's data with third parties and what type or categories of data are shared in order to provide the service. Disclosing the categories of personal information that is shared with third parties is not qualitatively better or worse because it is often a necessary requirement to share data to provide all the features of a product that includes sharing data with third-party service providers. A company should disclose what types of personal data are shared with third parties to ensure users have adequate notice if only some types or all of their data will be shared with third parties in order to provide informed consent.

Transparent Practice

The categories of information shared with third parties are indicated.

Statutes & Regulations:

- COPPA: (A parent or guardian can request the operator to provide a description of the specific types or categories of personal information collected from children by the application or service.) [129]
- CCPA: (A business shall disclose the category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed consumers' personal information for a business purpose, it shall disclose that fact.) [130]

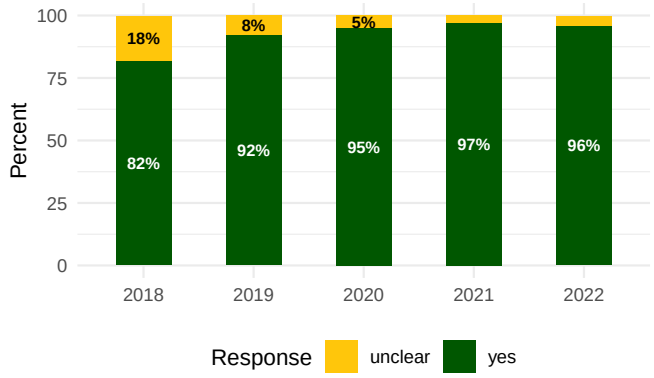
[129] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.6(a)(1).
[130] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.115(c)(2).

Data Use by Third Parties

3.2.1: Sharing Purpose

Do the policies clearly indicate the company's intention or purpose for sharing a user's personal information with third parties?

Figure 31: Sharing Purpose



The Sharing Purpose evaluation question indicates why a user's personal information is shared with third parties. A company should disclose the reasons why personal information is shared with third parties because it provides users with notice of how their data could be used by other companies, which could increase risk if used for unintended purposes.

Transparent Practice

The purpose for sharing a user's personal information with third parties is indicated.

Statutes & Regulations:

- COPPA: (An operator may share data with third parties who provide support for the "internal operations" of the service and who do not use or disclose the information for any other purpose.) [131]
- SOPIPA: (An operator is prohibited from sharing student information to third parties except in limited circumstances to other schools, or for research purposes.) [132]
- SOPIPA: (An operator may share student data with third parties for legitimate research purposes if not used for advertising or to amass a profile on a student for purposes other than K–12 school purposes.) [133]
- SOPIPA: (An operator may disclose student information to a third party service provider, but the third party is prohibited from using the information for or any purpose other than providing the service.) [134]
- GDPR: (Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: ... (d) where the processing is based on consent ... the legitimate interests pursued by the controller or by a third party.) [135]
- GDPR: (The controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: ... (b) where the processing is based on consent ... the legitimate interests pursued by the controller or by a third party.) [136]
- CCPA: ("Business purpose" means the use of personal information for the business's operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected.) [137]

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

[132] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4).

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

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

[135] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(1)(d).

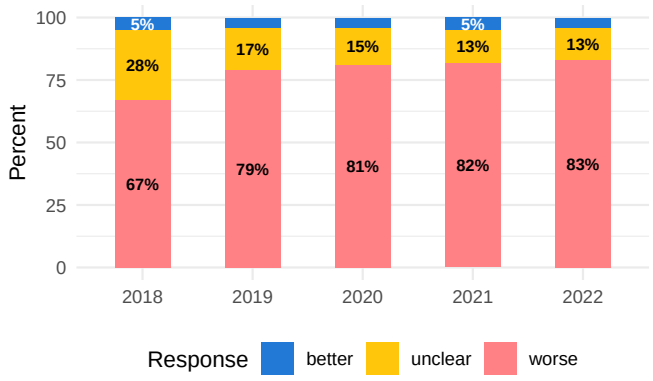
[136] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(b).

[137] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e).

3.2.2: Third-Party Analytics

Do the policies clearly indicate whether or not any information is shared with third parties for analytics purposes?

Figure 32: Third-Party Analytics



The Third-Party Analytics evaluation question indicates whether the product automatically collects usage data from a user based on their use of the product and then shares that data with a third-party analytics provider to better understand how their service is used. A company should disclose the name of any third-party analytics services that receive a user's data and take steps to minimize the amount of data sent to third parties for analytics purposes, which could increase risk if used for unintended purposes.

Better Practice

Data are not shared for analytics.

Worse Practice

Data are shared for analytics.

Statutes & Regulations:

- COPPA: (Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.) [138]
- SOPIPA: (An operator is prohibited from amassing a profile of a student.) [139]
- GDPR: (Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited unless: ... (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes ... which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.) [140]
- CCPA: (Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.) [141]

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

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

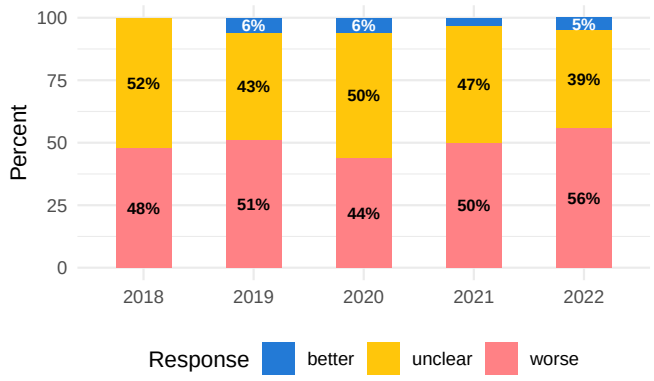
[140] *See* General Data Protection Regulation (GDPR) 2016/679, Processing of special categories of personal data, Art. 9(1)-(2)(j).

[141] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e)(5).

3.2.3: Third-Party Research

Do the policies clearly indicate whether or not any information is shared with third parties for research or product improvement purposes?

Figure 33: Third-Party Research



The Third-Party Research evaluation question indicates whether any information is disclosed to third parties for their own research purposes. A company should disclose what types of personal data are used for testing or research purposes because this practice is not the primary purpose of providing the product to users, and the risk of third parties re-identifying previously de-identified or anonymized data could be used for unintended purposes. However, companies can mitigate these risks by de-identifying or anonymizing children's and students' personal information before sharing with a third-party company or research institution and placing contractual limits on those companies of their use of the data.

Better Practice

Data are not shared for research and/or product improvement.

Worse Practice

Data are shared for research and/or product improvement.

Statutes & Regulations:

- COPPA: (Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.) [142]
- FERPA: (An exception for disclosing personally identifiable information without obtaining parental consent exists for sharing data with third parties conducting legitimate research and studies.) [143]
- SOPIPA: (An operator may share student data with third parties for legitimate research purposes if not used for advertising or to amass a profile on a student for purposes other than K–12 school purposes.) [144]
- SOPIPA: (An operator is prohibited from sharing student information to third parties except in limited circumstances to other schools, or for research purposes.) [145]
- PPRA: (All instructional materials including teacher's manuals, films, tapes, or other supplementary instructional material which is used in connection with any research must be made available for inspection by the parents or guardians of the children.) [146]
- CalPPR: (A school district may provide, in its discretion, statistical data from which no pupil may be identified to any public agency, entity, private nonprofit college, university, or educational research and development organization when disclosure would be in the best educational interests of pupils.) [147]
- CCPA: ("Research" means scientific analysis, systematic study and observation, including basic research or applied research that is designed to develop or contribute to public or scientific knowledge and that adheres or otherwise conforms to all other applicable ethics and privacy laws, including but not limited to studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall follow specified requirements.) [148]

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

[143] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(6); See also 34 C.F.R. Part 99.31(b)(2).

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

[145] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4).

[146] Protection of Pupil Rights Act (PPRA), 34 C.F.R. §98.3.

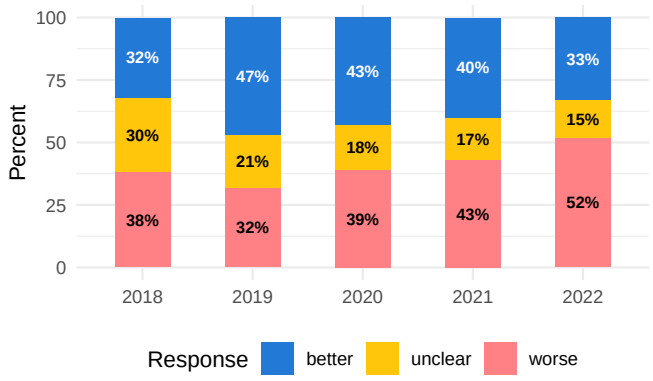
[147] California Privacy of Pupil Records, Cal. Ed. Code § 49074.

[148] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ab).

3.2.4: Third-Party Marketing

Do the policies clearly indicate whether or not personal information is shared with third parties for marketing purposes?

Figure 34: Third-Party Marketing



The Third-Party Marketing evaluation question indicates whether marketing communications that could include emails, text messages, or other notifications are sent to users are from an application or service that a user does not have a direct relationship with and therefore has different expectations, because it communicates unrelated or unsolicited products and features from third-party companies.

Better Practice

Personal information is not shared for third-party marketing.

Worse Practice

Personal information is shared for third-party marketing.

Statutes & Regulations:

- COPPA: (Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.) [149]
- ShineTheLight: (California's "Shine the Light" refers to information sharing disclosure requirements for companies that do business with California residents to allow customers to opt-out of information sharing, or make a detailed disclosure of how personal information was shared for direct marketing purposes.) [150]
- CalPRMDW: (Prohibits an operator from marketing or advertising non age-appropriate types of products or services to a minor under 18 years of age and from knowingly using, disclosing, compiling, or allowing a third party to use, disclose, or compile, the personal information of a minor for the purpose of marketing or advertising non age-appropriate types of products or services. Also, a minor is permitted to request to "erase" or remove and obtain removal of content or information posted on the operator's site.) [151]
- CCPA: ("Advertising and marketing" means a communication by a business or a person acting on the business's behalf in any medium intended to induce a consumer to obtain goods, services, or employment.) [152]
- CCPA: (A "business purpose" means providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer, provided that for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers which the service provider or contractor receives from or on behalf of the business with personal information which the service provider or contractor receives from or on behalf of another person or persons, or collects from its own interaction with consumers.) [153]

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

[150] Information Sharing Disclosure, Cal. Civ. Code §§ 1798.83-1798.84.

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

[152] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(a).

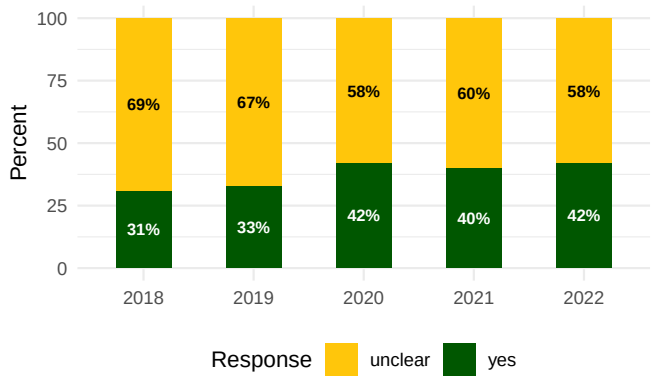
[153] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e)(6).

Data Not Shared With Third Parties

3.3.1: Exclude Sharing

Do the policies specify any types of categories of collected information that will not be shared with third parties?

Figure 35: Exclude Sharing



The Exclude Sharing evaluation question indicates whether specific types of personal information or information from a particular type of user that are collected by the product are excluded from sharing with third parties, because of a concern for the sensitive nature of the information. A company should not share personal information from users with third parties if disclosure is not required to provide the service. This best practice ensures users have better protection of their most sensitive personal information because it minimizes disclosure to third parties that could use the data for unintended purposes.

Transparent Practice

Specific categories of information are not shared with third parties.

Statutes & Regulations:

- CalOPPA: (An operator is required to identify the categories of third parties with whom the operator may share personally identifiable information.) [154]
- GDPR: (Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: ... (e) the recipients or categories of recipients of the personal data, if any.) [155]
- GDPR: (Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: ... (e) the recipients or categories of recipients of the personal data, where applicable.) [156]
- GDPR: (The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: ... (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations.) [157]

[154] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(1).

[155] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(1)(e).

[156] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(1)(e).

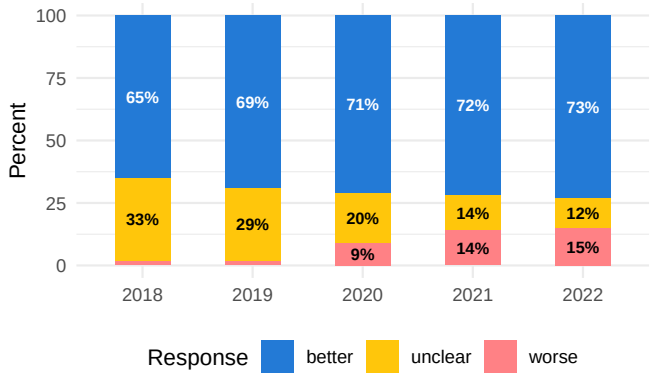
[157] General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(1).

Data Sold to Third Parties

3.4.1: 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 36: Sell Data



The Sell Data evaluation question indicates whether the policies disclose 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 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.

Better Practice

Personal information is not sold or rented to third parties.

Worse Practice

Personal information is sold or rented to third parties.

Statutes & Regulations:

- COPPA: (Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.) [158]
- SOPIPA: (An operator is prohibited from selling or renting student information.) [159]
- CCPA: (A consumer shall have the right to request that a business that sells or shares the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer: (1) The categories of personal information that the business collected about the consumer. (2) The categories of personal information that the business sold or shared about the consumer and the categories of third parties to whom the personal information was sold or shared, by category or categories of personal information for each category of third parties to whom the personal information was sold or shared. (3) The categories of personal information that the business disclosed about the consumer for a business purpose and the categories of persons to whom it was disclosed for a business purpose.) [160]
- CCPA: (A business that sells or shares personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose that information to the consumer upon receipt of a verifiable consumer request from the consumer. A business that sells or shares consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, the category or categories of consumers' personal information it has sold or shared, or if the business has not sold or shared consumers' personal information, it shall disclose that fact.) [161]
- CCPA: (A business that sells consumers' personal information to, or shares it with, third parties shall provide notice to consumers that this information may be sold or shared and that consumers have the "right to opt-out" of the sale or sharing of their personal information. A business shall not sell or share the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.) [162]
- CCPA: (A business that sells or shares consumers' personal information or uses or discloses consumers' sensitive personal information shall provide a clear and conspicuous link on the business's internet homepage(s), titled "Do Not Sell or Share My Personal Information," to an internet webpage that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or sharing of the consumer's personal information.) [163]
- CCPA: ("Sell," "selling," "sale," or "sold," means 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

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

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

[160] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.115(a)(1)-(3).

[161] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.115(b)-(c)(1).

[162] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.120(b)-(c).

[163] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.135(a).

a third party for monetary or other valuable consideration.) [164]

- CAADCA: (A business shall not collect, sell, share, or retain any personal information or precise geolocation information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, unless the business can demonstrate a compelling reason that the collecting, selling, sharing, or retaining of the personal information is in the best interests of children.) [165]
- GDPR: (The controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: ... (b) the existence of the right to ... object to processing.) [166]
- GDPR: (The controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: ... (c) the existence of the right to ... object to processing.) [167]
- GDPR: (The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: ... (e) the existence of the right to... object to processing.) [168]
- GDPR: (The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: ... (d) the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.) [169]

[164] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ad)(1).

[165] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(b)(3),(5).

[166] *See* General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(2)(b).

[167] *See* General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(c.)

[168] *See* General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(1)(e).

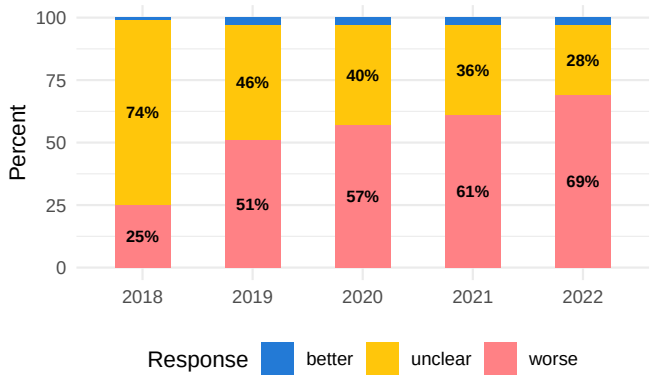
[169] *See* General Data Protection Regulation (GDPR) 2016/679, Right to restriction of processing, Art. 18(1)(d).

Third-Party Data Acquisition

3.5.1: Data Obtained

Do the policies clearly indicate whether or not the company may obtain a user's information from a third party?

Figure 37: Data Obtained



The Data Obtained evaluation question indicates whether personal information is purchased or acquired by the company from third-party companies such as data brokers to augment or supplement the data the company already collects from individual users to further personalize the service. A company should disclose whether data about a user is acquired from other sources than the product because it increases risk that a user's data may be used for unintended purposes.

Better Practice

Personal information about users is not obtained from third parties.

Worse Practice

Personal information about users is obtained from third parties.

Statutes & Regulations:

- CalOPPA: (An operator is required to identify the categories of personally identifiable information that they collect about individual consumers who use or visit its website or online service.) [170]
- CalOPPA: (The term "Personally Identifiable Information" under CalOPPA means individually identifiable information about a consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following: (1) A first and last name; (2) A home or other physical address, including street name and name of a city or town; (3) An e-mail address; (4) A telephone number; (5) A social security number; or (6) Any other identifier that permits the physical or online contacting of a specific individual.) [171]
- GDPR: (The controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: ... (f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources.) [172]
- GDPR: (The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: ... (g) where the personal data are not collected from the data subject, any available information as to their source.) [173]
- CCPA: (A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the categories of sources from which the personal information is collected.) [174]
- CCPA: (A business shall disclose in its privacy policy the categories of sources from which consumers' personal information is collected;.) [175]
- CCPA: ("Personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this paragraph, "publicly available" means: information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. "Personal information" does not include consumer information that is deidentified or aggregate consumer information.) [176]

[170] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(1).

[171] *See* California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22577(a)(1)-(6).

[172] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(f).

[173] General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(1)(g).

[174] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.110(a)(2).

[175] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.130(a)(5)(B)(ii).

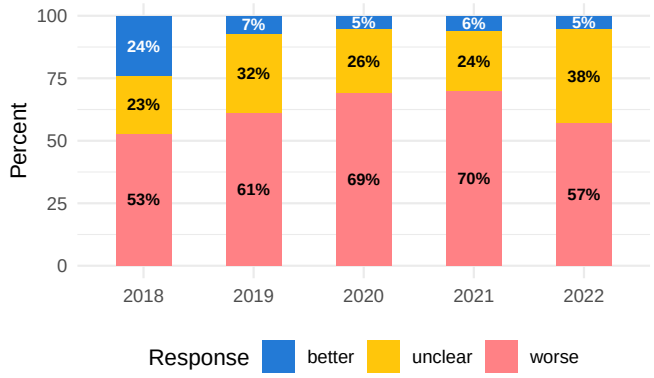
[176] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(v)(2).

Third-Party Links

3.6.1: Outbound Links

Do the policies clearly indicate whether or not outbound links on the product to third-party external resources are age-appropriate?

Figure 38: Outbound Links



The Outbound Links evaluation question indicates whether notice is provided to the user if they interact with hyperlinks, buttons, or other actions that cause the user to leave the product to access third-party content or resources that may not be age-appropriate. A company should notify users about any actions taken that cause them to leave the product and potentially subject themselves to different third-party privacy practices or age-inappropriate content.

Better Practice

Links to third-party external websites are age-appropriate.

Worse Practice

Links to third-party external websites are not age-appropriate.

Statutes & Regulations:

- CIPA: (If an operator provides third-party links on its site that link to potentially non-age appropriate information for children, then the operator must provide notice upon clicking a third-party link that a user is leaving the website.) [177]

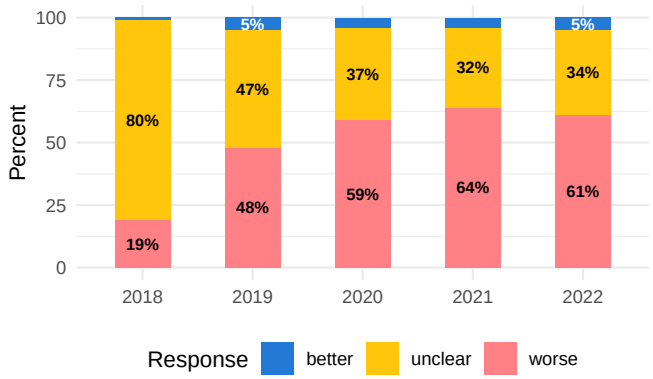
[177] Children's Internet Protection Act (CIPA), 47 U.S.C. § 254.

Third-Party Data Access

3.7.1: Authorized Access

Do the policies clearly indicate whether or not any third party is authorized to access a user's information?

Figure 39: Authorized Access



The Authorized Access evaluation question indicates whether the product allows the integration of third-party services to access a user's personal information collected by the product to provide additional features or plugins. A company should disclose the names of any third-party services that may access a user's information because it increases the risk that a user's data may be used for unintended purposes.

Better Practice

Third parties are not authorized to access a user's information.

Worse Practice

Third parties are authorized to access a user's information.

Statutes & Regulations:

- CalOPPA: (An operator is required to identify the categories of third parties with whom the operator may share personally identifiable information.) [178]

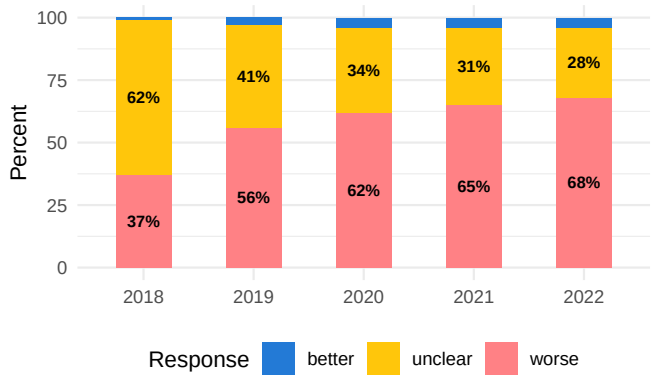
[178] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(1).

Third-Party Data Collection

3.8.1: Third-Party Collection

Do the policies clearly indicate whether or not a user's personal information is collected by a third party?

Figure 40: Third-Party Collection



The Third-Party Collection evaluation question indicates whether the product allows the integration of third-party services to collect a user's personal information when using the product to provide additional features. A company should disclose the names of any third-party services that may collect a user's information because it increases the risk that a user's data may be used for unintended purposes.

Better Practice

Personal information of users is not collected by a third party.

Worse Practice

Personal information of users is collected by a third party.

Statutes & Regulations:

- CalOPPA: (An operator is required to disclose whether other third parties may collect personally identifiable information about a consumer's online activities over time and across different Websites.) [179]

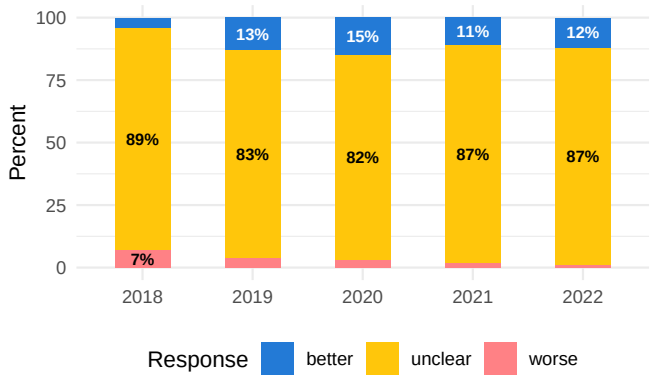
[179] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(6).

Third-Party Data Misuse

3.9.1: Third-party Deletion

Do the policies clearly indicate whether or not a user's information can be deleted from a third party?

Figure 41: Third-party Deletion



The Third-party Deletion evaluation question indicates whether a user's personal information may be deleted or restricted from a third-party service provider. A company should ensure that any of their users' data that is shared with a third party may also be deleted.

Better Practice

Personal information can be deleted from a third party.

Worse Practice

Personal information cannot be deleted from a third party.

Statutes & Regulations:

- CCPA: (A business that collects a consumer's personal information and that sells or shares personal information with a third party or that discloses it to a service provider or contractor for a business purpose shall enter into an agreement that grants the business the right to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.) [180]
- CCPA: (A business is required to monitor a third-party contractor's compliance through measures including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months.) [181]
- AB 1584: (A local educational agency that enters into a contract with a third party must ensure the contract contains a statement that pupil records continue to be the property of and under the control of the local educational agency.) [182]

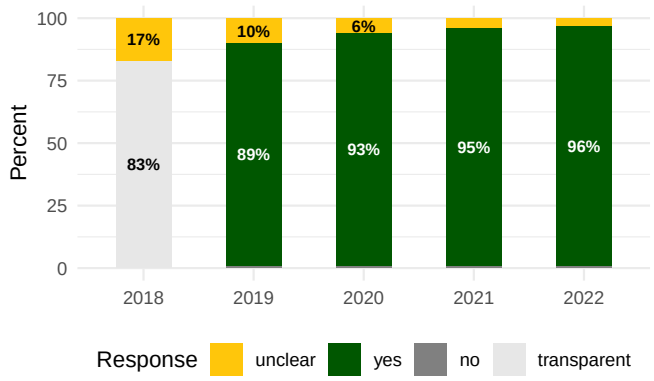
[180] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100(d)(5).
[181] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(j)(1)(C).
[182] California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(1).

Third-Party Service Providers

3.10.1: Third-Party Providers

Do the policies clearly indicate whether or not third-party services are used to support the company's product?

Figure 42: Third-Party Providers



The Third-Party Providers evaluation question indicates whether the product uses third-party service providers to support the product or service. It is important that companies disclose whether they use third-party service providers in order to allow parents and educators to easily determine where their data is processed and stored for compliance and accountability purposes. With increased globalization and ubiquitous availability of cloud and support services, it is sometimes difficult to determine where a child or student's personal information is actually processed and stored.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

- COPPA: (Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.) [183]
- COPPA: (An operator may share data with third parties who provide support for the "internal operations" of the service and who do not use or disclose the information for any other purpose.) [184]
- SOPIPA: (An operator may disclose student information to a third party service provider, but the third party is prohibited from using the information for or any purpose other than providing the service.) [185]
- CCPA: (A business that receives a verifiable consumer request shall disclose any personal information it has collected about a consumer, directly or indirectly to the consumer. A service provider or contractor shall not be required to comply with a verifiable consumer request received directly from a consumer or a consumer's authorized agent to the extent that the service provider or contractor has collected personal information about the consumer in its role as a service provider or contractor. A service provider or contractor shall provide assistance to a business with which it has a contractual relationship with respect to the business's response to a verifiable consumer request, including but not limited to by providing to the business the consumer's personal information in the service provider or contractor's possession, which the service provider or contractor obtained as a result of providing services to the business, and by correcting inaccurate information, or by enabling the business to do the same. A service provider or contractor that collects personal information pursuant to a written contract with a business shall be required to assist the business through appropriate technical and organizational measures taking into account the nature of the processing.) [186]
- CCPA: ("Contractor" means a person to whom the business makes available a consumer's personal information for a business purpose pursuant to a written contract with the business, provided that the contract follow specified requirements.) [187]
- CCPA: ("Service provider" means a person that processes personal information on behalf of a business and which receives from or on behalf of the business a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the person from specified requirements.) [188]
- GDPR: (Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: ... (e) the recipients or categories of recipients of the personal data, where applicable.) [189]

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

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

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

[186] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.130(a)(3)(A).

[187] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(j)(1).

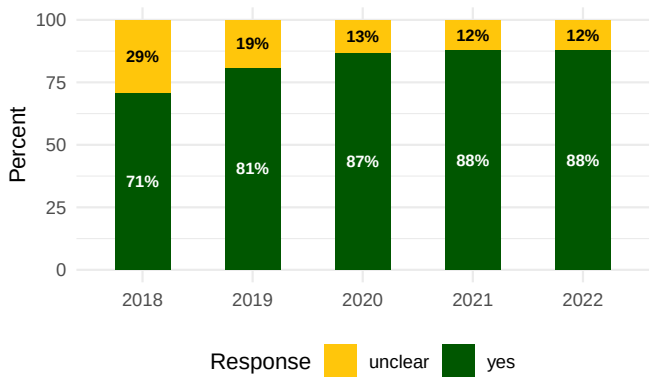
[188] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ag)(1).

[189] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(1)(e).

3.10.2: Third-Party Roles

Do the policies clearly indicate the role or purpose of third-party service providers?

Figure 43: Third-Party Roles



The Third-Party Roles evaluation question indicates the purpose of a third-party service provider. It is important for a company to clearly explain and define the role third parties have in supporting the internal operations of the company's product. It is not sufficient to state that a third party is used without also clarifying how that third party uses shared information. Clarifying the role of third parties helps parents and educators make a more informed decision by better understanding the reason the company is using third-party service providers. This information is necessary to balance the risk of sharing data against the value of the additional services provided and the compliance obligations to disclose the roles of third-party providers.

Transparent Practice

The roles of third-party service providers are indicated.

Statutes & Regulations:

- COPPA: (An operator may share data with third parties who provide support for the "internal operations" of the service and who do not use or disclose the information for any other purpose.) [190]
- SOPIPA: (An operator may disclose student information to a third party service provider, but the third party is prohibited from using the information for or any purpose other than providing the service.) [191]
- CCPA: (Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.) [192]

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

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

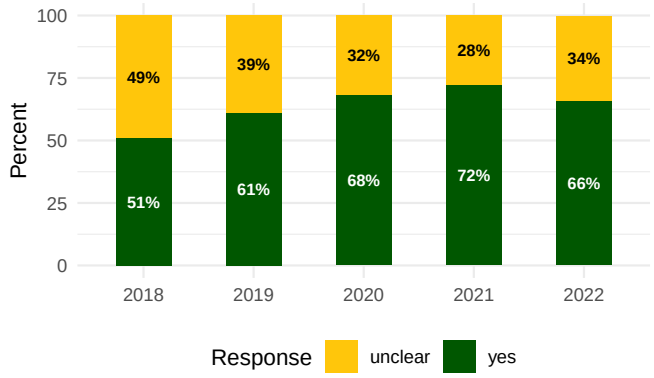
[192] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e)(5).

Third-Party Affiliates

3.11.1: Related Third-Party

Do the policies clearly indicate the categories of related third parties, such as subsidiaries or affiliates with whom the company shares data?

Figure 44: Related Third-Party



The Related Third-Party evaluation question indicates the types and names of third-party companies such as affiliates, subsidiaries, or partners that a product shares a user's data with for purposes unrelated to providing the service. It is important for a company to clearly explain and define the role of third parties that have access to users' data but provide no support for the internal operations of the company's product. It is not sufficient to state that a user's data is shared with a related third party without also clarifying how that third party uses the shared information. Clarifying the role of related third parties helps parents and educators make a more informed decision by better understanding the purpose of the company sharing data with different categories of third parties.

Transparent Practice

The categories of third parties that receive data are indicated.

Statutes & Regulations:

- CalOPPA: (An operator is required to identify the categories of third parties with whom the operator may share personally identifiable information.) [193]
- GDPR: (Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: ... (e) the recipients or categories of recipients of the personal data, if any.) [194]
- GDPR: (Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: ... (e) the recipients or categories of recipients of the personal data, where applicable.) [195]
- GDPR: (The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: ... (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations.) [196]
- CCPA: (A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the categories of third parties to whom the business discloses personal information.) [197]
- CCPA: (A "business" includes any entity that controls or is controlled by a business and that shares common branding with the business and with whom the business shares consumers' personal information. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark, such that the average consumer would understand that two or more entities are commonly owned. A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.) [198]

[193] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(1).

[194] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(1)(e).

[195] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(1)(e).

[196] General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(1).

[197] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.110(a)(4).

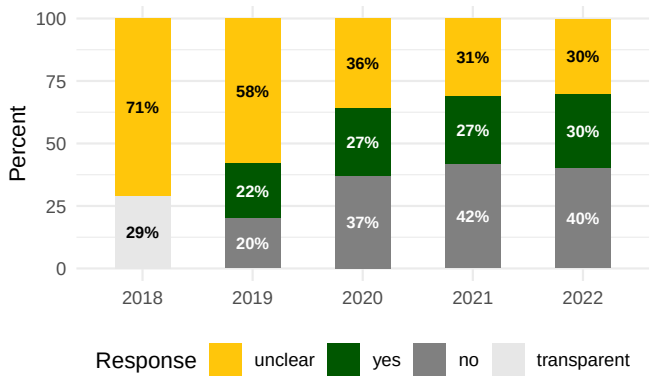
[198] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(d)(2)-(3).

Third-Party Policies

3.12.1: Third-Party Policy

Do the policies clearly indicate whether or not privacy policy links are provided to any third-party service provider, data processor, partner, or affiliate?

Figure 45: Third-Party Policy



The Third-Party Policy evaluation question indicates whether notice is provided of any privacy policy links or URLs for any third-party service providers or third-party companies that may access a user's personal information. A company should disclose links to the privacy policies of any third-party company that the product may share a user's personal information with so users can make a more informed decision by better understanding the privacy practices of the third parties who may access their data.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

- CCPA: (A business that is acting as a third party and controls the collection of personal information about a consumer shall inform consumers by providing the required information prominently and conspicuously on the homepage of its internet website.) [199]

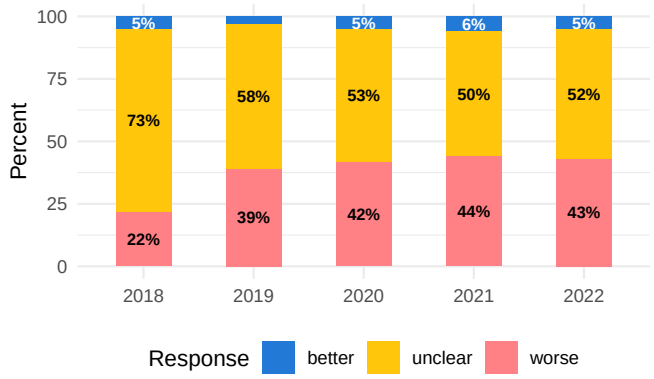
[199] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100(b).

Third-Party Data Combination

3.13.1: Company Combination

Do the policies clearly indicate whether or not data collected or maintained by the first-party company can be augmented, extended, or combined with data from third-party sources?

Figure 46: Company Combination



The Company Combination evaluation question indicates whether information collected from the product is combined with other information acquired by the company from third-party sources. A company should disclose whether a user's data is augmented or supplemented because the risk could increase if the combined data is used by the company or third parties for unintended purposes.

Better Practice

Company will not combine data with additional data from third-party sources.

Worse Practice

Company may combine data with additional data from third-party sources.

Statutes & Regulations:

- COPPA: (Non-personal information collected from a child that is later combined with personally identifiable information of that child, obtained from either the vendor or third party becomes PII.) [200]
- GDPR: ("processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.) [201]

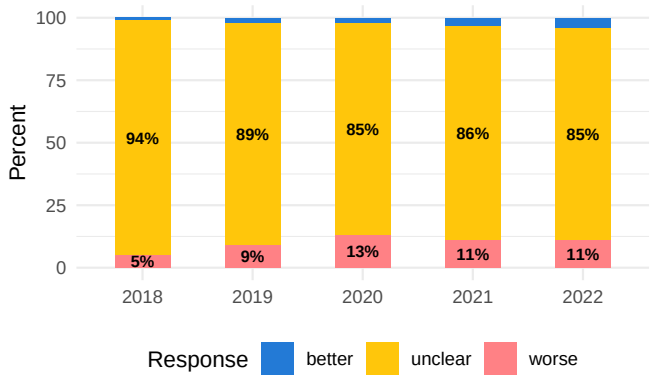
[200] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

[201] *See* General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(2).

3.13.2: Third-Party Combination

Do the policies clearly indicate whether or not data shared with third-party companies can be augmented, extended, or combined with data from any source?

Figure 47: Third-Party Combination



The Third-Party Combination evaluation question indicates whether third parties may combine a user's information shared with them by a first-party company that has a direct relationship with their user with other information acquired from other third-party sources. A company should place contractual restrictions on third-party companies that receive users' personal information from the product because of the increased risk the combined data is used for unintended purposes.

Better Practice

Data shared with third parties cannot be combined with other data.

Worse Practice

Data shared with third parties can be combined with other data.

Statutes & Regulations:

- COPPA: (Non-personal information collected from a child that is later combined with personally identifiable information of that child, obtained from either the vendor or third party becomes PII.) [202]
- SOPIPA: (An operator may disclose student information to a third party service provider, but the third party is prohibited from using the information for or any purpose other than providing the service.) [203]
- CCPA: (A “business purpose” means providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer, provided that for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers which the service provider or contractor receives from or on behalf of the business with personal information which the service provider or contractor receives from or on behalf of another person or persons, or collects from its own interaction with consumers.) [204]
- CCPA: (“Contractor” means a person to whom the business makes available a consumer's personal information for a business purpose pursuant to a written contract with the business, provided that the contract prohibits the contractor from selling or sharing the personal information; Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract; or Combining the personal information which the contractor receives pursuant to a written contract.) [205]

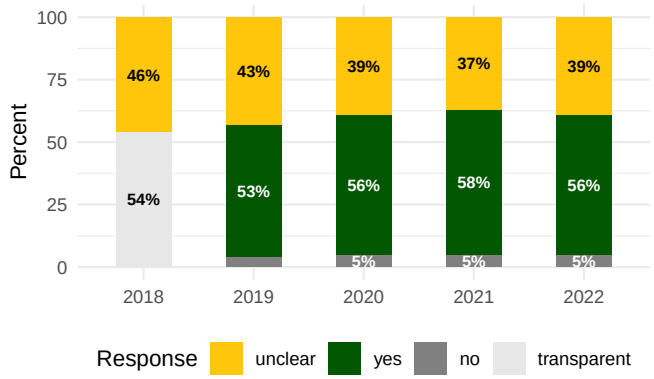
[202] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.
[203] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4)(E)(i).
[204] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e)(6).
[205] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(j)(1)(A)(i)-(iv).

Third-Party Authentication

3.14.1: Third-Party Login

Do the policies clearly indicate whether or not any third-party, social, or federated login is supported to use the product?

Figure 48: Third-Party Login



The Third-Party Login evaluation question indicates whether the product incorporates a third-party service provider's federated or social login feature to authenticate users with the product. It is becoming increasingly difficult for consumers, parents, and educators to manage the proliferation of all the different applications and services they use themselves, and by their children and students on a daily basis. In order to streamline the account-creation process, outsource account management, and outsource authorization practices, many companies have incorporated social or federated login options into their products. However, third-party login services may collect a user's data from their use of the product over time, and third-party login providers may have different data collection and use privacy practices, which can increase the risk that a user's data is used for unintended purposes.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

- COPPA: (An operator may share data with third parties who provide support for the "internal operations" of the service and who do not use or disclose the information for any other purpose.) [206]
- SOPIPA: (An operator may disclose student information to a third party service provider, but the third party is prohibited from using the information for or any purpose other than providing the service.) [207]
- CCPA: (Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.) [208]

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

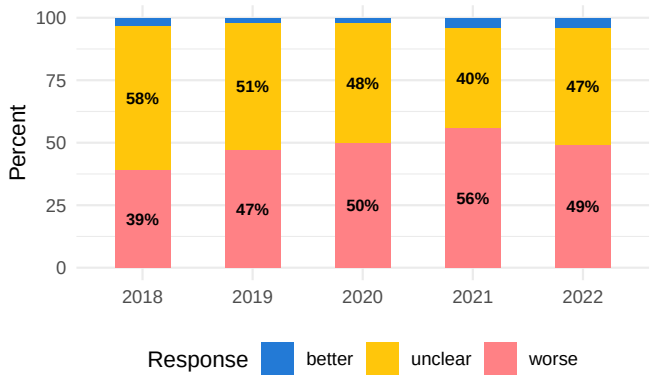
[207] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4)(E)(i).

[208] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e)(5).

3.14.2: Login Collection

Do the policies clearly indicate whether or not the company collects any information from any third-party login providers?

Figure 49: Login Collection



The Login Collection evaluation question indicates whether the product collects personal information from the integration of a third-party login provider that could be used to augment or supplement a user's personal information collected by the product. A "better" response to this evaluation question indicates the product does not collect personal information from third-party login providers about users.

Better Practice

Personal information from third-party login providers is not collected.

Worse Practice

Personal information from third-party login providers is collected.

Statutes & Regulations:

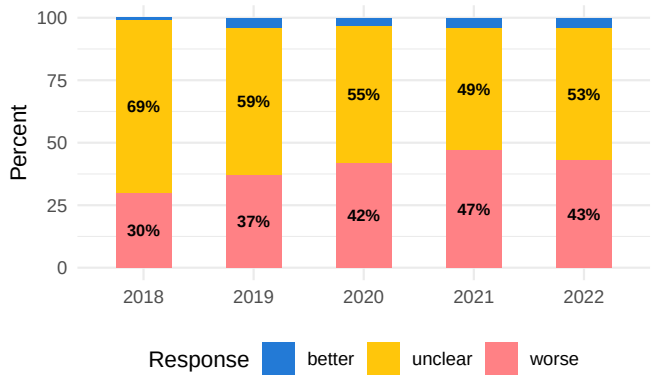
- CalPPR: (Prohibits schools, school districts, county offices of education, and charter schools from collecting or maintaining information about pupils from social media for any purpose other than school or pupil safety, without notifying each parent or guardian and providing the pupil with access and an opportunity to correct or delete such information.) [209]

[209] California Privacy of Pupil Records, Cal. Ed. Code § 49073.6(c).

3.14.3: Login Sharing

Do the policies clearly indicate whether or not the company shares any information with third-party login providers?

Figure 50: Login Sharing



The Login Sharing evaluation question indicates whether the product may disclose personal information collected from the product with a third-party login provider. A company should disclose whether data about a user can be shared with third-party login providers because it increases risk that a user's data may be used for unintended purposes.

Better Practice

Personal Information is not shared with third-party login providers.

Worse Practice

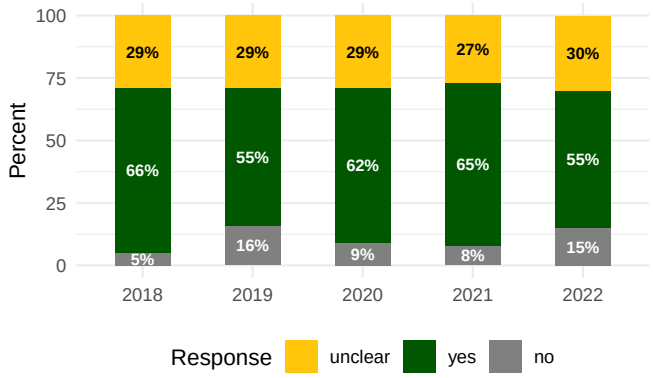
Personal Information is shared with third-party login providers.

De-identified or Anonymized Data

3.15.1: Data De-identified

Do the policies clearly indicate whether or not a user's information that is shared or sold to a third-party is only done so in an anonymous or de-identified format?

Figure 51: Data De-identified



The Data De-identified evaluation question indicates whether a user's personal information is disclosed with third parties if the data is de-identified or anonymized by the company before it is shared. Disclosing collected information in an anonymous or de-identified format is a complicated issue and even data that has gone through this process can often be recombined with other data to allow re-identification with only a few known data points. As such, sharing of any information, even information about a user that has been de-identified or anonymized, is a privacy risk.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

- COPPA: (An operator may disclose personal information collected from children to third parties if the data is not in an identifiable form such as de-identified, aggregated, or anonymous information.) [210]
- FERPA: (An exception for disclosing personally identifiable information without obtaining parental consent exists for sharing "de-identified" student records where the educational institution has made a reasonable determination that a student's identity is not personally identifiable.) [211]
- SOPIPA: (An operator may share student information with a third party if in an aggregated or de-identified format.) [212]
- CalPPR: (A school district may provide, in its discretion, statistical data from which no pupil may be identified to any public agency, entity, private nonprofit college, university, or educational research and development organization when disclosure would be in the best educational interests of pupils.) [213]
- GDPR: (If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.) [214]
- CCPA: ("Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.) [215]
- CCPA: ("Deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that the business that possesses the information pursuant to specified requirements.) [216]
- CCPA: ("Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.) [217]
- CCPA: (A businesses shall not be restricted to collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information.) [218]
- Telecom Act: (A telecommunications carrier that receives or obtains customer proprietary network in-

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

[211] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(b)(1).

[212] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(f)-(g).

[213] California Privacy of Pupil Records, Cal. Ed. Code § 49074.

[214] *See* General Data Protection Regulation (GDPR) 2016/679, Processing which does not require identification, Art. 11(1).

[215] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(b).

[216] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(m).

[217] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(aa).

[218] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.145(a)(6).

formation may use, disclose, or permit access to aggregate customer information for any purpose.) [219]

- Telecom Act: (The term "aggregate customer information" means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.) [220]

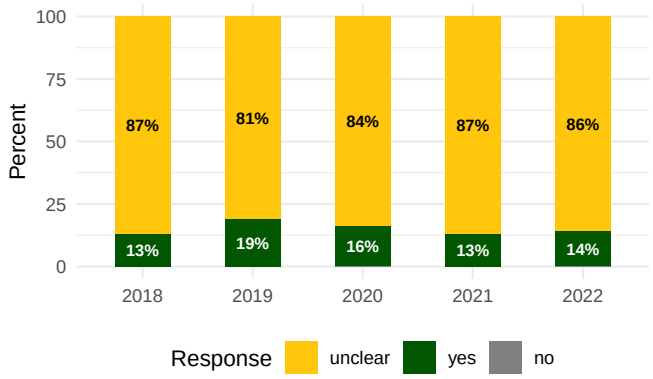
[219] Telecommunications Act, Privacy of customer information, 47 U.S. Code § 222(c)(3).

[220] Telecommunications Act, Privacy of customer information, 47 U.S. Code § 222(h)(1)(A).

3.15.2: De-identified Process

Do the policies clearly indicate whether or not the de-identification process is done with a reasonable level of justified confidence, or whether the company provides links to any information that describes their de-identification process?

Figure 52: De-identified Process



The De-identified Process evaluation question indicates whether a company provides notice of its de-identification or anonymization process of user data with a reasonable level of justified confidence that data cannot be re-identified by third parties. Companies should disclose that their de-identification or anonymization of personal information is completed in a manner such that personal data can no longer be attributed to a specific individual without the use of additional information. In addition, the company should describe or provide links to any technical and organizational measures they use to ensure that the personal data of their users are not attributed to a specific individual.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

- COPPA: (An operator may disclose personal information collected from children to third parties if the data is not in an identifiable form such as de-identified, aggregated, or anonymous information.) [221]
- FERPA: (An exception for disclosing personally identifiable information without obtaining parental consent exists for sharing "de-identified" student records where the educational institution has made a reasonable determination that a student's identity is not personally identifiable.) [222]
- SOPIPA: (An operator may share student information with a third party if in an aggregated or de-identified format.) [223]
- GDPR: ("pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.) [224]
- CCPA: ("Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.) [225]
- CCPA: ("Deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that the business that possesses the information takes reasonable measures to ensure that the information cannot be associated with a consumer or household.) [226]

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

[222] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(b)(1).

[223] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(f)-(g).

[224] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(5).

[225] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(b).

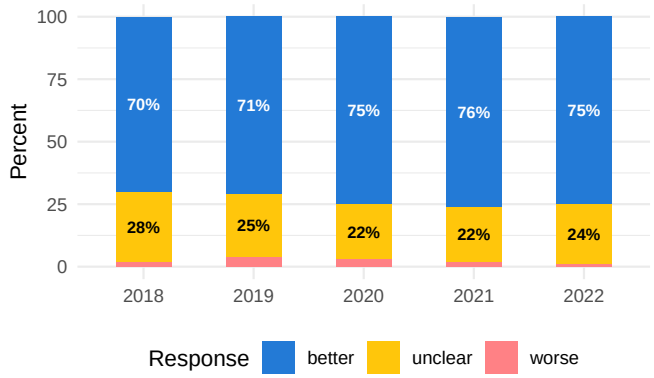
[226] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(m)(A).

Third-Party Contractual Obligations

3.16.1: Third-Party Limits

Do the policies clearly indicate whether or not the company imposes contractual limits on how third parties can use personal information that the company shares or sells to them?

Figure 53: Third-Party Limits



The Third-Party Limits evaluation question indicates whether the company has placed contractual obligations on any third-party companies that receive a user's data from the product. A company should put in place contractual obligations that require third parties to only collect and use that data in accordance with the company's privacy policy. Without contractual limits on third-party use of data, parents and educators cannot reasonably expect that the privacy practices outlined in the product's policies will be honored by third parties that have access to personal data.

Better Practice

Contractual limits are placed on third-party data use.

Worse Practice

Contractual limits are not placed on third-party data use.

Statutes & Regulations:

- COPPA: (An operator must take reasonable steps to release a child's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of the information, and provide assurances that they contractually maintain the information in the same manner.) [227]
- FERPA: (An exception for disclosing personally identifiable information without obtaining parental consent exists for sharing data with a third party who is considered a “school official” with a legitimate educational interest, and under direct control of the school for the use and maintenance of education records.) [228]
- SOPIPA: (An operator may disclose student information to a third party service provider, but the third party is prohibited from using the information for or any purpose other than providing the service.) [229]
- SOPIPA: (A third party service provider may not disclose student information to any subsequent third party.) [230]
- GDPR: (The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.) [231]
- GDPR: (Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.) [232]
- GDPR: (Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor ... shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfill its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.) [233]
- GDPR: (The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller.) [234]
- CCPA: (A business shall enter into an agreement with a third party, service provider, or contractor, that specifies personal information that is sold or

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

[228] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(i)(B).

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

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

[231] General Data Protection Regulation (GDPR) 2016/679, Processor, Art. 28(2).

[232] General Data Protection Regulation (GDPR) 2016/679, Processor, Art. 28(3).

[233] General Data Protection Regulation (GDPR) 2016/679, Processor, Art. 28(4).

[234] General Data Protection Regulation (GDPR) 2016/679, Processing under the authority of the controller or processor, Art. 29

disclosed by the business is only for limited and specified purposes and the third party shall provide the same level of privacy protection.)[235]

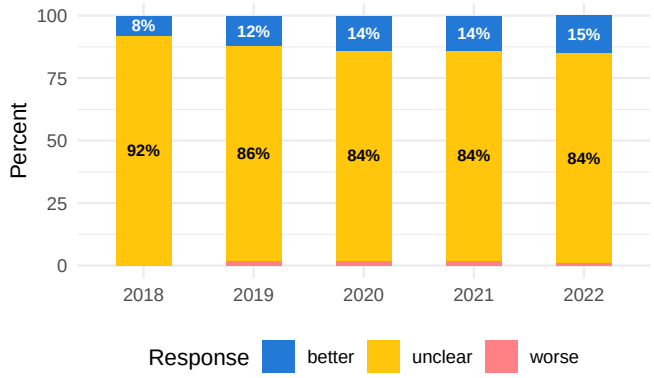
- CCPA: (A business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into an agreement with that third party to not sell or share personal information about a consumer that has been sold to, or shared with, the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out.)[236]
- CCPA: (A service provider or contractor that assists a business may not use the sensitive personal information, after it has received instructions from the business and to the extent it has actual knowledge that the personal information is sensitive personal information for any other purpose. A service provider or contractor is only required to limit its use of sensitive personal information received pursuant to a written contract with the business in response to instructions from the business and only with respect to its relationship with that business.)[237]
- CCPA: ("Contractor" means a person to whom the business makes available a consumer's personal information for a business purpose pursuant to a written contract with the business, provided that the contract prohibits the contractor from selling or sharing the personal information; Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract; or Combining the personal information which the contractor receives pursuant to a written contract.)[238]
- CCPA: (If a contractor engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the contractor engages another person to assist in processing personal information for such business purpose, it shall notify the business of such engagement and the engagement shall be pursuant to a written contract.)[239]
- CCPA: ("Deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, provided that the business that possesses the information publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision; and contractually obligates any recipients of the information.)[240]

[235] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100(d)(1)-(4).
[236] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.115(d).
[237] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.121(c).
[238] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(j)(1)(A)(i)-(iv).
[239] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(j)(2).
[240] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(m)(B)-(C).

3.16.2: Combination Limits

Do the policies clearly indicate whether or not the company imposes contractual limits that prohibit third parties from reidentifying or combining data with other data sources that the company shares or sells to them?

Figure 54: Combination Limits



The Combination Limits evaluation question indicates whether the company has placed contractual prohibitions or restrictions on any third-party companies that receive a user's data from the product for re-identification of anonymized or de-identified data. A company should put in place contractual prohibitions that require third parties to not attempt to combine, augment or supplement acquired third-party data about a user with a user's first-party data that has been shared with them by the company, or attempt reidentification of any users in anonymized or de-identified data.

Better Practice

Contractual limits prohibit third parties from reidentifying or de-identified information.

Worse Practice

Contractual limits do not prohibit third parties from reidentifying or de-identified information.

Statutes & Regulations:

- COPPA: (An operator must take reasonable steps to release a child's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of the information, and provide assurances that they contractually maintain the information in the same manner.) [241]
- CCPA: (Sensitive Personal information that is collected or processed without the purpose of inferring characteristics about a consumer shall be treated as personal information for purposes of all other sections of this Act.) [242]
- CCPA: ("Contractor" means a person to whom the business makes available a consumer's personal information for a business purpose pursuant to a written contract with the business, provided that the contract prohibits the contractor from selling or sharing the personal information; Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract; or Combining the personal information which the contractor receives pursuant to a written contract.) [243]

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

[242] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.121(d).

[243] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(j)(1)(A)(i)-(iv).

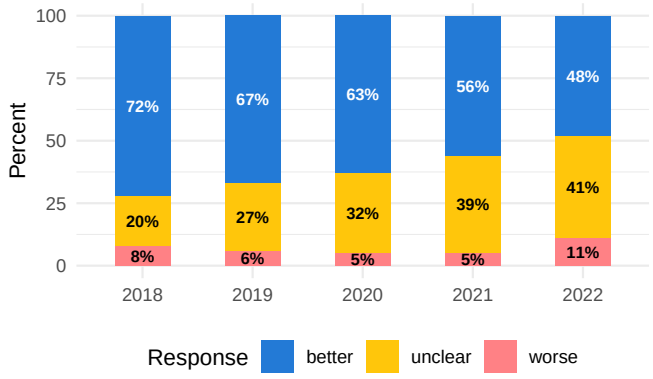
Respect for Context (What are the Data Purpose, Classification, Notice, and Changes?)

Data Use

4.1.1: Purpose Limitation

Do the policies clearly indicate whether or not the company limits the use of data collected by the product to the purpose of providing the service?

Figure 55: Purpose Limitation



The Purpose Limitation evaluation question indicates whether the company limits the use of data collected by the product to only the purpose of providing the service. The purpose of collection can vary between the type of product and type of user if a product's purpose is for educational, entertainment, or content delivery purposes. A company should disclose the purpose for which personal data is collected by the product because there is an increased risk if the data is used for unintended purposes not related to providing the services.

Better Practice

Use of information is limited to the purpose for which it was collected.

Worse Practice

Use of information is not limited to the purpose for which it was collected.

Statutes & Regulations:

- COPPA: (An operator may retain information collected from a child only as long as necessarily to fulfill the purpose for which it was collected and must delete the information using reasonable measures to prevent unauthorized use.) [244]
- COPPA: (An operator is required to provide direct notice to parents describing what information is collected, how information is used, its disclosure practices and exceptions.) [245]
- SOPIPA: ("K–12 school purposes" means purposes that customarily take place at the direction of the K–12 school, teacher, or school district or aid in the administration of school activities, including instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school.) [246]
- AB 1584: (A local educational agency that enters into a contract with a third party must ensure the contract contains a prohibition against the third party using any information in the pupil record for any purpose other than those required or specifically permitted by the contract.) [247]
- GDPR: (Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.) [248]
- GDPR: (The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.) [249]
- CCPA: (A business's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was

[244] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.10.
[245] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(b).
[246] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(j)
[247] California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(3).
[248] General Data Protection Regulation (GDPR) 2016/679, Principles relating to processing of personal data, Art. 5(1)(b).
[249] General Data Protection Regulation (GDPR) 2016/679, Data protection by design and by default, Art. 25(2).

collected, and not further processed in a manner that is incompatible with those purposes.) [250]

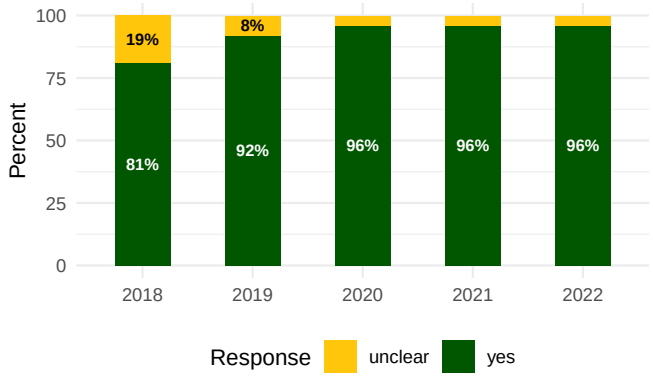
- CCPA: ("Business purpose" means the use of personal information for the business's operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected.) [251]
- CAADCA: (A business that provides an online service, product, or feature likely to be accessed by children shall not use the personal information of any child in a way that the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of a child.) [252]
- Telecom Act: (A telecommunications carrier that receives or obtains customer proprietary network information shall only use, disclose, or permit access to individually identifiable customer proprietary network information to provide the telecommunications service.) [253]
- CCPA: ("Business purpose" means the use of personal information for the business's operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected.) [254]

[250] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100(c).
[251] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e).
[252] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(b)(1).
[253] Telecommunications Act, Privacy of customer information, 47 U.S. Code § 222(c)(1).
[254] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e)(2)-(3).

4.1.2: Data Purpose

Do the policies clearly indicate the context or purpose for which data are collected?

Figure 56: Data Purpose



The Data Purpose evaluation question indicates the context and reason why a user's personal information is collected by the product and the purpose for which it will be used to provide the service. A company should disclose the reasons it collects different types of data in order to help parents and educators make an informed decision whether to use the product, because it provides users with a better understanding of the purpose for which their data is collected and used.

Transparent Practice

The context or purpose for which data are collected is indicated.

Statutes & Regulations:

- GDPR: (Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: ... (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.) [255]
- GDPR: (Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.) [256]
- GDPR: (The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: ... (a) the purposes of the processing.) [257]
- CCPA: (A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the business or commercial purpose for collecting, selling, or sharing personal information.) [258]
- CCPA: (A business shall disclose the category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed consumers' personal information for a business purpose, it shall disclose that fact.) [259]
- CCPA: ("Business purpose" means the use of personal information for the business's operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected.) [260]

[255] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(1)(c).

[256] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(1)(c).

[257] General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(1)(a).

[258] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.110(a)(3).

[259] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.115(c)(2).

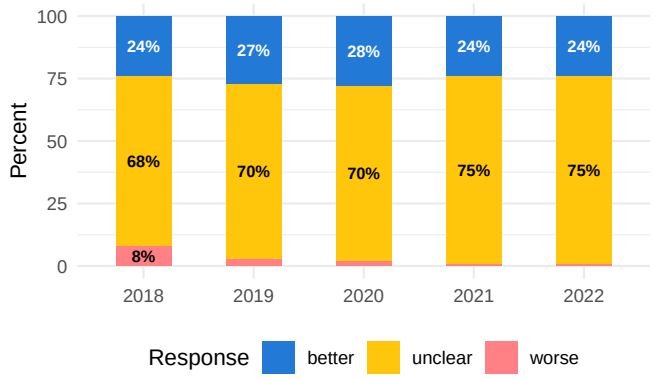
[260] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e).

Data Combination

4.2.1: Combination Type

Do the policies clearly indicate whether or not the company treats personal information combined with non-personally identifiable information as personal information?

Figure 57: Combination Type



The Combination Type evaluation question indicates the type of information data is considered if it is combined with personally identifiable information (PII). A company should be aware of the risks of combining personally identifiable information (PII) collected by the product with automatically collected non-personally identifiable information or acquired data from third parties. If a user's personal information is combined with any other type of data, the augmented or supplemented data should be treated as PII because of the additional protections given to this data type under federal and state privacy laws.

Better Practice

Combined information is treated as personally identifiable information (PII).

Worse Practice

Combined information is not treated as personally identifiable information (PII).

Statutes & Regulations:

- COPPA: (Non-personal information collected from a child that is later combined with personally identifiable information of that child, obtained from either the vendor or third party becomes PII.) [261]

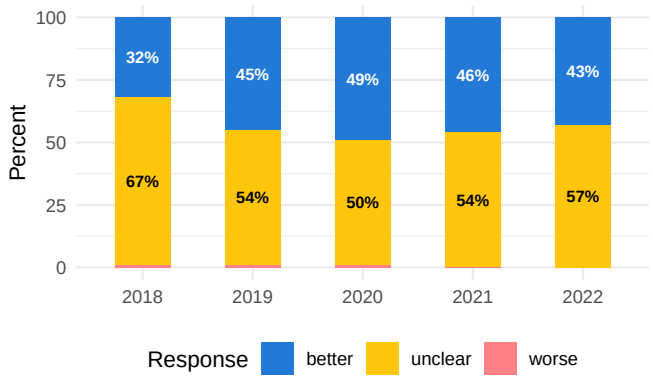
[261] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

Data Notice

4.3.1: Context Notice

Do the policies clearly indicate whether or not notice is provided to a user if the company changes the purpose or context in which data are collected?

Figure 58: Context Notice



The Context Notice evaluation question indicates whether notice is given to users if the purpose or context for which their data is collected or used changes from a user's reasonable expectation. A company that intends to process a user's personal information for a different purpose than the data was originally collected for should provide the user with notice of the change in context for the new and additional purpose.

Better Practice

Notice is provided if the context in which data are collected changes.

Worse Practice

Notice is not provided if the context in which data are collected changes.

Statutes & Regulations:

- GDPR: (Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose.)[262]
- GDPR: (Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose.)[263]
- CCPA: (A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether such information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, without providing the consumer with notice. If the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used and whether such information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected, without providing the consumer with notice.)[264]
- CCPA: (A business's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.)[265]
- CCPA: ("Business purpose" means the use of personal information for the business's operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected.)[266]
- CCPA: ("Business purpose" means the use of personal information for the business's operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected.)[267]

[262] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(3).

[263] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, GDPR Art. 14(4).

[264] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100(a)(1)-(2).

[265] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100(c).

[266] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e).

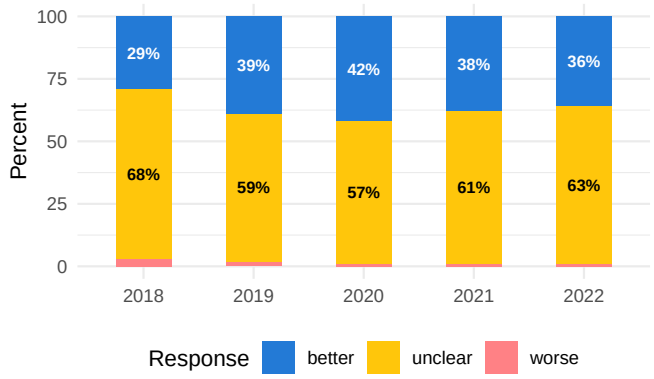
[267] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e)(2)-(3).

Data Changes

4.4.1: Context Consent

Do the policies clearly indicate whether or not the company obtains consent if the practices in which a user's data are collected change or are inconsistent for the purpose in which it was collected?

Figure 59: Context Consent



The Context Consent evaluation question indicates whether informed consent is obtained from a user if the context or purpose in which their data is collected or used changes from the user's reasonable expectation. A company that intends to process a user's personal information for a different purpose than the data was originally collected should obtain consent for the change in context for the other purpose.

Better Practice

Consent is obtained if the practices in which data are collected change.

Worse Practice

Consent is not obtained if the practices in which data are collected change.

Statutes & Regulations:

- GDPR: (Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, several factors.) [268]

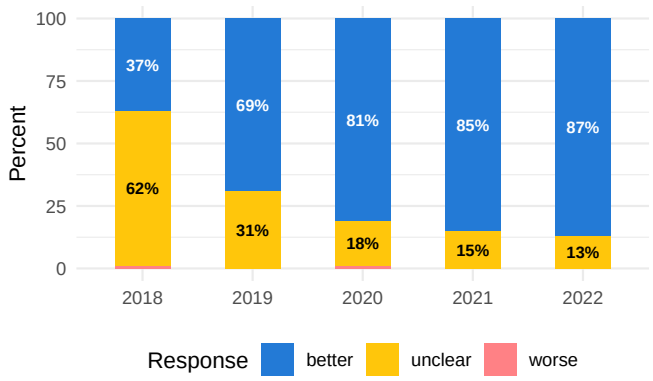
[268] General Data Protection Regulation (GDPR) 2016/679, Lawfulness of Processing, Art. 6(4)(a)-(d).

Policy Enforcement

4.5.1: Community Guidelines

Do the policies clearly indicate whether or not the company may terminate a user's account if they engage in any prohibited activities?

Figure 60: Community Guidelines



The Community Guidelines evaluation question indicates what type of user content or activities are prohibited on the product and clear examples to help the user understand what the rules are and how they are enforced. A company should disclose that violations of the rules may result in the restriction or termination of a user's account so all users have adequate notice of the product's rules and consequences to help provide a safer environment.

Better Practice

Accounts may be terminated if users engage in any prohibited activities.

Worse Practice

Accounts may not be terminated if users engage in any prohibited activities.

Statutes & Regulations:

- CAADCA: (A business shall enforce its published terms, policies, and community standards established by the business, including privacy policies and those concerning children.) [269]

[269] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(a)(9).

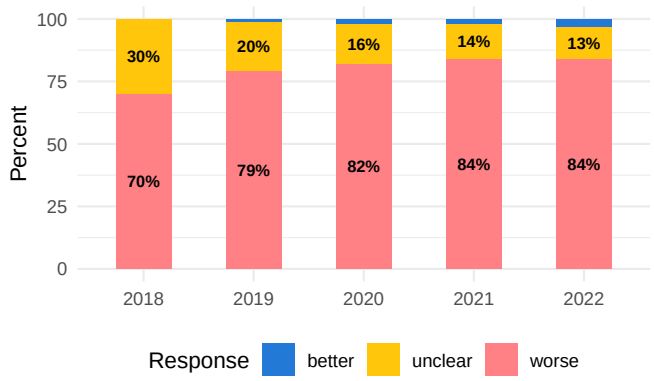
Individual Control (How are Data Owned, Licensed, Used, Disclosed, and Managed?)

User Content

5.1.1: User Submission

Do the policies clearly indicate whether or not a user can create or upload content to the product?

Figure 61: User Submission



The User Submission evaluation question indicates whether the user may create content or upload user-generated content to the product. User-generated content often contains personal, private, or sensitive information in text, audio, images, photographs, or video format that if inadvertently disclosed to third parties for unintended purposes could cause serious privacy risks and harms.

Better Practice

Users cannot create or upload content.

Worse Practice

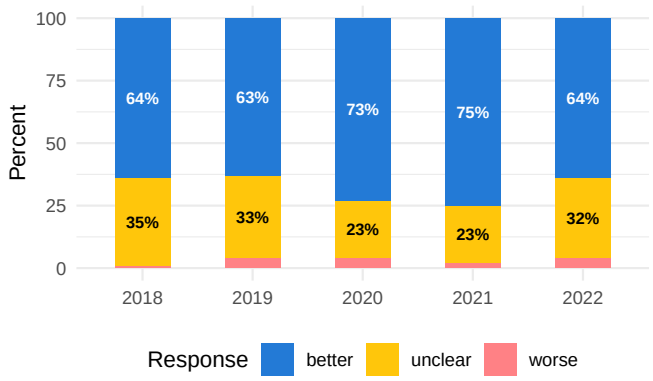
Users can create or upload content.

User Consent

5.2.1: Collection Consent

Do the policies clearly indicate whether or not the company obtains opt-in consent from a user at the time any information is collected?

Figure 62: Collection Consent



The Collection Consent evaluation question indicates whether the company requests opt-in consent from a user at the time personal information is collected with just-in-time or pop-up notices of what information will be collected and how it will be used. A company should provide notice to users in an easy-to-read format as a supplemental notice of the product's privacy policy at the point of collection in order to obtain better informed consent.

Better Practice

Opt-in consent is requested from users at the time personal information is collected.

Worse Practice

Opt-in consent is not requested from users at the time personal information is collected.

Statutes & Regulations:

- COPPA: (A notice or privacy policy on an operator's website needs a section relating to the collection of information for children under 13 years of age, and notice is required at each area of the site where information is collected from children.) [270]
- GDPR: ("consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.) [271]
- GDPR: (Processing shall be lawful only if and to the extent ... the data subject has given consent to the processing of his or her personal data for one or more specific purposes.) [272]
- GDPR: (Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.) [273]
- GDPR: (If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.) [274]
- CCPA: ("Consent" means any freely given, specific, informed and unambiguous indication of the consumer's wishes by which he or she, or his or her legal guardian, by a person who has power of attorney or is acting as a conservator for the consumer, such as by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.) [275]

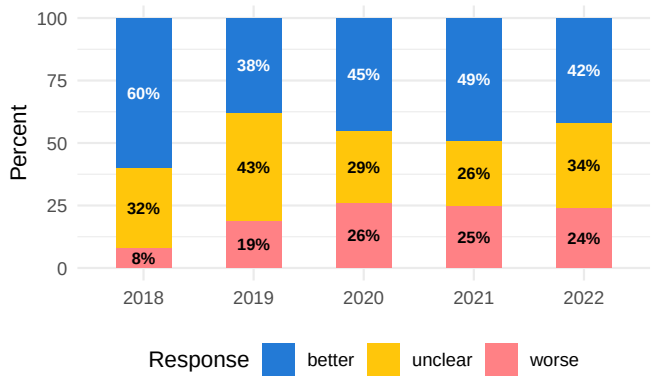
[270] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d).
[271] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(11).
[272] General Data Protection Regulation (GDPR) 2016/679, Lawfulness of Processing, Art. 6(1)(a).
[273] General Data Protection Regulation (GDPR) 2016/679, Conditions for Consent, Art. 7(1).
[274] General Data Protection Regulation (GDPR) 2016/679, Conditions for Consent, Art. 7(2).
[275] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(h).

Remedy Process

5.3.1: Complaint Notice

Do the policies clearly indicate whether or not the company has a grievance or remedy mechanism for users to file a complaint after the company restricts or removes a user's content or account?

Figure 63: Complaint Notice



The Complaint Notice evaluation question indicates whether notification is provided to users if their account or content is restricted and if users can file a complaint with the company against the account or content restriction. A company should provide notice of a dispute resolution process for any account or content that is restricted and any available remedies.

Better Practice

A grievance or remedy mechanism is available for users to file a complaint.

Worse Practice

A grievance or remedy mechanism is not available for users to file a complaint.

Statutes & Regulations:

- CDA: (No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or any action taken to enable or make available to information content providers or others the technical means to restrict access to material.) [276]
- DMCA: (The provider of a service or application that has removed or disabled access to material or activity claimed to be infringing must take reasonable steps to promptly notify the subscriber that it has removed or disabled access to their material.) [277]
- GDPR: ("restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future.) [278]
- GDPR: (The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: ... (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead.) [279]
- GDPR: (The controller shall communicate any ... restriction of processing... to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.) [280]
- GDPR: (The controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: ... (d) the right to lodge a complaint with a supervisory authority.) [281]
- GDPR: (The controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: (e) the right to lodge a complaint with a supervisory authority.) [282]
- GDPR: (The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: ... (f) the right to lodge a complaint with a supervisory authority.) [283]
- GDPR: (Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as

[276] The Communications Decency Act of 1996 (CDA), 47 U.S.C. 230(c).

[277] Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512(g)(2)(A).

[278] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(3).

[279] General Data Protection Regulation (GDPR) 2016/679, Right to restriction of processing, Art. 18(1)(b).

[280] General Data Protection Regulation (GDPR) 2016/679, Notification obligation regarding rectification or erasure of personal data or restriction of processing, Art. 19.

[281] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(2)(d).

[282] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(e).

[283] General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(1)(f).

a result of the processing of his or her personal data in non-compliance with this Regulation.) [284]

- GDPR: (Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.) [285]
- DSA: (Providers of online platforms shall suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide manifestly illegal content.) [286]
- DSA: (Providers of hosting services shall provide a clear and specific statement of reasons to any affected recipients of the service for any restrictions imposed on the ground that the information provided by the recipient of the service is illegal content or incompatible with their terms and conditions.) [287]
- DSA: (Providers of online platforms shall provide recipients of the service, including individuals or entities that have submitted a notice, with access to an effective internal complaint-handling system that enables them to lodge complaints, electronically and free of charge, against the decision taken by the provider of the online platform upon the receipt of a notice or against the following decisions taken by the provider of the online platform on the grounds that the information provided by the recipients constitutes illegal content or is incompatible with its terms and conditions.) [288]

[284] General Data Protection Regulation (GDPR) 2016/679, Right to an effective judicial remedy against a controller or processor, Art. 79(1).

[285] General Data Protection Regulation (GDPR) 2016/679, Right to an effective judicial remedy against a controller or processor, Art. 79(2).

[286] Digital Services Act (Regulation (EU) 2022/2065), Measures and protection against misuse, Art. 23.

[287] Digital Services Act (Regulation (EU) 2022/2065), Statement of reasons, Art. 17.

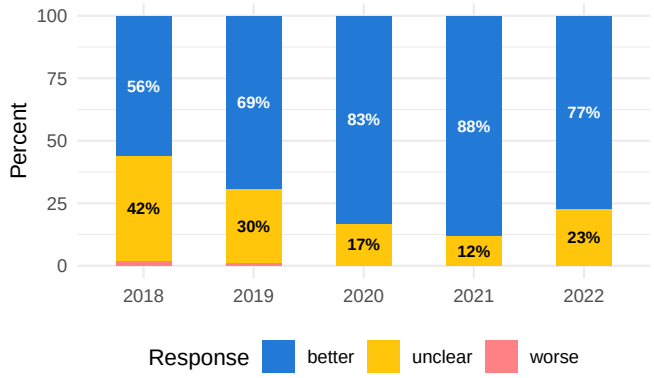
[288] Digital Services Act (Regulation (EU) 2022/2065), Internal complaint-handling system, Art. 20.

Data Settings

5.4.1: Privacy Settings

Do the policies clearly indicate whether or not a user can control the use of their information through privacy settings?

Figure 64: Privacy Settings



The Privacy Settings evaluation question indicates whether users can control the use of their information in the product through changes in processing, privacy controls, or product settings. A company should provide information about a product's privacy settings and controls that users have with their personal information in a company's policies before users provide their data to a product, not afterward.

Better Practice

Users can control the use of their information through privacy settings.

Worse Practice

Users cannot control the use of their information through privacy settings.

Statutes & Regulations:

- CAADCA: (A business shall configure all default privacy settings provided to children by the online service, product, or feature to settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children.) [289]
- DSA: (Providers of online platforms shall not design, organize or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions.) [290]
- CCPA: ("Consent" means any freely given, specific, informed and unambiguous indication of the consumer's wishes by which he or she, or his or her legal guardian, by a person who has power of attorney or is acting as a conservator for the consumer, such as by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.) [291]
- CCPA: ("Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation.) [292]
- CAADCA: (A business shall not use dark patterns to encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being.) [293]

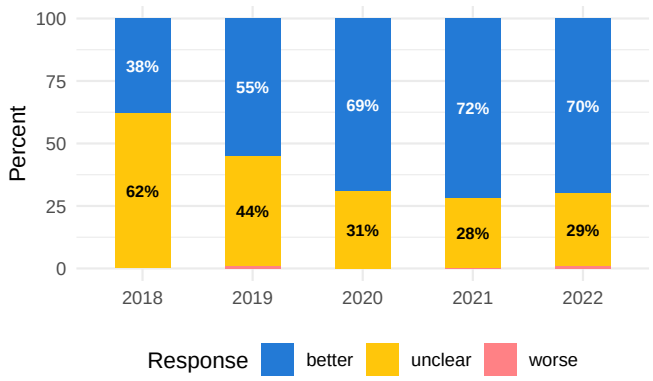
[289] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(a)(6).
[290] Digital Services Act (Regulation (EU) 2022/2065), Online interface design and organization, Art. 25.
[291] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(h).
[292] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(l).
[293] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(b)(7).

Data Disclosure

5.5.1: Opt-Out Consent

Do the policies clearly indicate whether or not a user can opt out from the disclosure or sale of their data to a third party?

Figure 65: Opt-Out Consent



The Opt-Out Consent evaluation question indicates whether a user can opt out or object to the company's processing of their information for a particular purpose such as selling data to third parties. A company should respect a user's informed consent and choice that the product must change its data collection, use, or disclosure practices of the personal information with respect to that user.

Better Practice

Users can opt out from the disclosure or sale of their data to a third party.

Worse Practice

Users cannot opt out from the disclosure or sale of their data to a third party.

Statutes & Regulations:

- ShineTheLight: (California's "Shine the Light" refers to information sharing disclosure requirements for companies that do business with California residents to allow customers to opt-out of information sharing, or make a detailed disclosure of how personal information was shared for direct marketing purposes.) [294]
- GDPR: (The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.) [295]
- GDPR: (The controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: ... (b) the existence of the right to ... object to processing.) [296]
- GDPR: (The controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: ... (c) the existence of the right to ... object to processing.) [297]
- GDPR: (The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: ... (e) the existence of the right to... object to processing.) [298]
- GDPR: (The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: ... (c) the data subject objects to the processing ... and there are no overriding legitimate grounds for the processing.) [299]
- GDPR: (The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her ... including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.) [300]
- GDPR: (At the latest at the time of the first communication with the data subject, the right to object ... shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.) [301]
- CCPA: (A business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into an agreement

[294] Information Sharing Disclosure, Cal. Civ. Code §§ 1798.83-1798.84.

[295] General Data Protection Regulation (GDPR) 2016/679, Conditions for Consent, Art. 7(3).

[296] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(2)(b).

[297] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(c.)

[298] General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(1)(e).

[299] General Data Protection Regulation (GDPR) 2016/679, Right to erasure, Art. 17(1)(c.)

[300] General Data Protection Regulation (GDPR) 2016/679, Right to object, Art. 21(1).

[301] General Data Protection Regulation (GDPR) 2016/679, Right to object, Art. 21(4).

with that third party to not sell or share personal information about a consumer that has been sold to, or shared with, the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out.) [302]

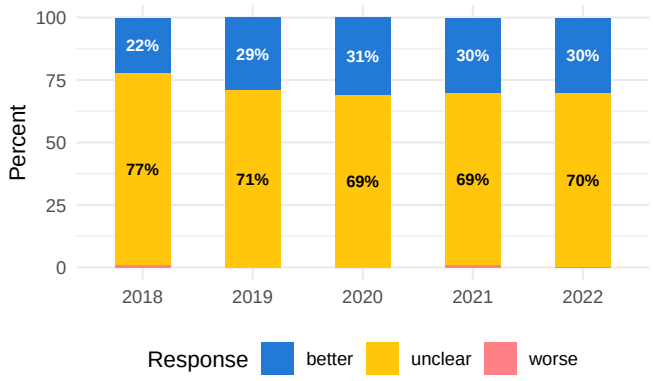
- CCPA: (A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. This right may be referred to as the right to opt-out of sale or sharing.) [303]
- CCPA: (A business that has received direction from a consumer not to sell or share the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell or share the minor consumer's personal information, shall be prohibited from selling or sharing the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides consent, for the sale or sharing of the consumer's personal information.) [304]
- CCPA: (A business that sells or shares consumers' personal information or uses or discloses consumers' sensitive personal information shall in a form that is reasonably accessible to consumers provide a clear and conspicuous link on the business's internet homepage(s), titled "Do Not Sell or Share My Personal Information," to an internet webpage that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or sharing of the consumer's personal information. A business shall not be required to comply if the business allows consumers to opt-out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism to the business indicating the consumer's intent to opt-out of the business's sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information, or both.) [305]
- CCPA: (A business shall not use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt- out request.) [306]
- CAADCA: (The term "default" means a preselected option adopted by the business for the online service, product, or feature.) [307]
- DSA: (Providers of online platforms that use recommender systems shall set out in their terms and conditions, in plain and intelligible language, the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters.) [308]

[302] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.115(d).
[303] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.120(a).
[304] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.120(d).
[305] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.135(a)-(b).
[306] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.135(c)(6).
[307] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.30(b)(3).
[308] Digital Services Act (Regulation (EU) 2022/2065), Recommender system transparency, Art. 27.

5.5.2: Disclosure Request

Do the policies clearly indicate whether or not a user can request the company to provide all the personal information the company has shared with third parties?

Figure 66: Disclosure Request



The Disclosure Request evaluation question indicates whether users can obtain notice of what personal information the company shared with third parties. A company should respond to a user's request and provide notice of whether a user's personal information was disclosed to third parties because there is an increased risk a user's personal information may be used for unintended purposes.

Better Practice

Users can request to know what personal information has been shared with third parties.

Worse Practice

Users can not request to know what personal information has been shared with third parties.

Statutes & Regulations:

- ShineTheLight: (California's "Shine the Light" refers to information sharing disclosure requirements for companies that do business with California residents to allow customers to opt-out of information sharing, or make a detailed disclosure of how personal information was shared for direct marketing purposes.) [309]
- FERPA: (A parent or guardian may request to receive a copy of their student's records that have been disclosed by the vendor.) [310]
- GDPR: (The controller shall take appropriate measures to provide any information ... relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.) [311]
- GDPR: (The controller shall provide information on action taken on a request ... to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.) [312]
- GDPR: (If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.) [313]
- GDPR: (Information provided ... and any communication and any actions taken ... shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.) [314]
- GDPR: (The information to be provided to data subjects may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.) [315]

[309] Information Sharing Disclosure, Cal. Civ. Code §§ 1798.83-1798.84.

[310] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30(c)(1).

[311] *See* General Data Protection Regulation (GDPR) 2016/679, Transparent information communication and modalities for the exercise of the rights of the data subject, Art. 12(1).

[312] *See* General Data Protection Regulation (GDPR) 2016/679, Transparent information, communication and modalities for the exercise of the rights of the data subject, Art. 12(3).

[313] *See* General Data Protection Regulation (GDPR) 2016/679, Transparent information, communication and modalities for the exercise of the rights of the data subject, Art. 12(4.)

[314] *See* General Data Protection Regulation (GDPR) 2016/679, Transparent information, communication and modalities for the exercise of the rights of the data subject, Art. 12(5).

[315] *See* General Data Protection Regulation (GDPR) 2016/679, Transparent information, communication and modalities for the exercise of the rights of the data subject, Art. 12(7).

- GDPR: (The controller shall provide the information ... (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.) [316]
- GDPR: (Notice shall not apply where and insofar as: ... (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or in so far as the obligation of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.) [317]
- CCPA: (A business that sells or shares consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose the category or categories of consumers' personal information it has sold or shared, or if the business has not sold or shared consumers' personal information, it shall disclose that fact.) [318]
- CCPA: ((iii) the business or commercial purpose for collecting or selling or sharing consumers' personal information; and (iv) the categories of third parties to whom the business discloses consumers' personal information.) [319]

[316] *See* General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(3)(a)-(c).

[317] *See* General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(5)(b).

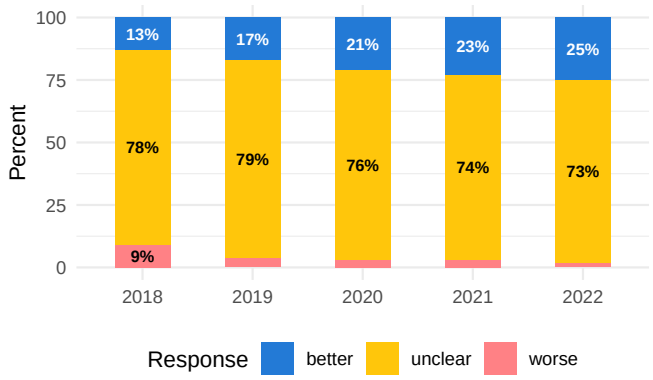
[318] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.115(c)(1)-(2).

[319] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.130(a)(5)(B)(iii).

5.5.3: Disclosure Notice

Do the policies clearly indicate whether or not the company will provide the affected user with notice in the event the company receives a government or legal request for their information?

Figure 67: Disclosure Notice



The Disclosure Notice evaluation question indicates whether notification is provided to an affected user of a government or private company request for their personal information collected from the product. A company should disclose the number of legal requests for information received and situations when the company might not notify users, including a description of the types of government requests it is prohibited by law from disclosing to users.

Better Practice

Notice is provided in the event the company receives a government or legal request for a user's information.

Worse Practice

Notice is not provided in the event the company receives a government or legal request for a user's information.

Statutes & Regulations:

- FERPA: (An educational agency or institution may disclose information for lawful reasons if they make a reasonable effort to notify the parent or eligible student of the order or subpoena in advance of compliance, so that the parent or eligible student may seek protective action.) [320]
- CalECPA: (Prohibits a government entity from compelling the production of or access to electronic communication information or electronic device information, without a search warrant, wiretap order, order for electronic reader records, or subpoena issued under specified conditions, except for emergency situations.) [321]
- GDPR: (The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: ... (d) the personal data have been unlawfully processed.) [322]
- GDPR: (The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: ... (d) the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.) [323]

[320] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(9)(ii).

[321] California Electronic Communications Privacy Act, Cal. Pen. Code § 1546-1546.4.

[322] *See* General Data Protection Regulation (GDPR) 2016/679, Right to erasure, Art. 17(1)(d).

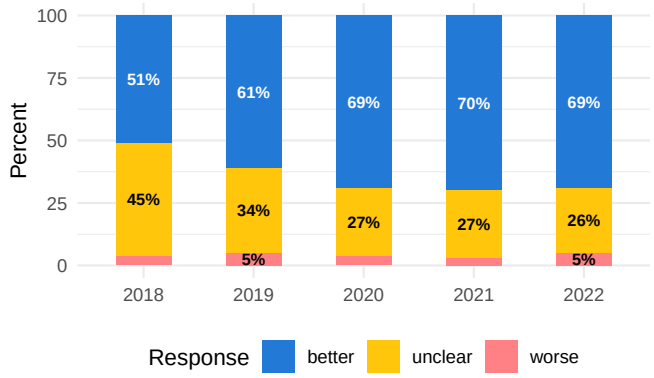
[323] *See* General Data Protection Regulation (GDPR) 2016/679, Right to restriction of processing, Art. 18(1)(d).

Intellectual Property

5.6.1: Data Ownership

Do the policies clearly indicate whether or not a user retains ownership to the Intellectual Property rights of the data collected or uploaded to the product?

Figure 68: Data Ownership



The Data Ownership evaluation question indicates whether the user retains copyright authorship or ownership rights to the user-generated content created or uploaded by the user to the product. A company should respect the intellectual property rights of the content creators using its service and allow users to extend copyright protection to their works.

Better Practice

Users retain ownership of their data.

Worse Practice

Users do not retain ownership of their data.

Statutes & Regulations:

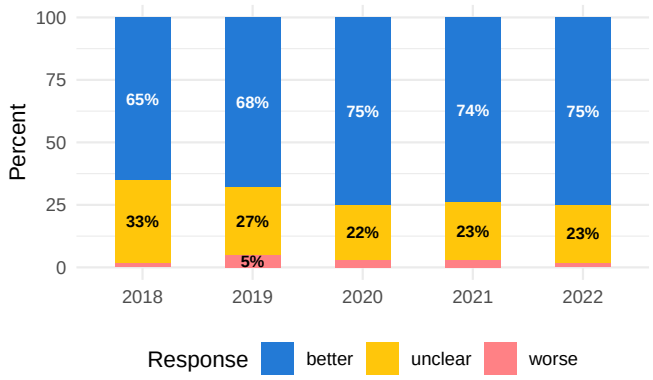
- AB 1584: (A local educational agency that enters into a contract with a third party must ensure the contract contains a statement that pupil records continue to be the property of and under the control of the local educational agency.) [324]
- Copyright: (Copyright protection is extended to original works of authorship fixed in any tangible medium of expression.) [325]

[324] California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(1).
[325] Copyright Act of 1976, 17 U.S.C. § 102.

5.6.2: Copyright License

Do the policies clearly indicate whether or not the company may claim a copyright license to the data or content collected from a user?

Figure 69: Copyright License



The Copyright License evaluation question indicates whether the company may claim a copyright license to a user's information or content that is created with or uploaded to the service. A company should respect the intellectual property rights of the content creators using its service and only claim a copyright license to a user's work in order to display and distribute the works for the purpose of providing the service.

Better Practice

A copyright license is claimed to data or content collected from a user.

Worse Practice

A copyright license is not claimed to data or content collected from a user.

Statutes & Regulations:

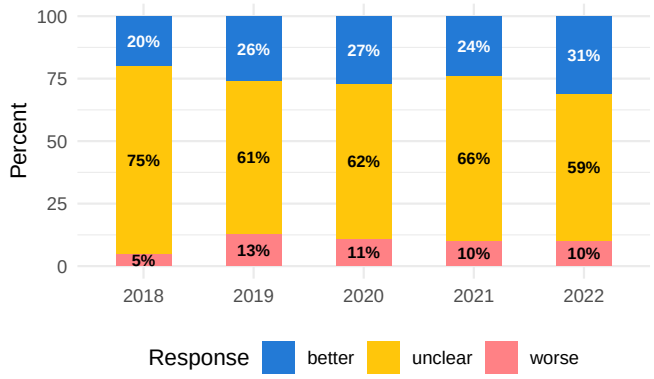
- Copyright: (Copyright protection is extended to original works of authorship fixed in any tangible medium of expression.) [326]

[326] Copyright Act of 1976, 17 U.S.C. § 102.

5.6.3: Copyright Limits

Do the policies clearly indicate whether or not the company limits its copyright license of a user's data?

Figure 70: Copyright Limits



The Copyright Limits evaluation question indicates that the company limits or terminates its copyright license to a user's information or content created with the product in certain situations, such as when information or content is deleted from the service or after a specified period of account inactivity.

Better Practice

Any copyright license to a user's data is limited in scope or duration.

Worse Practice

Any copyright license to a user's data is not limited in scope or duration.

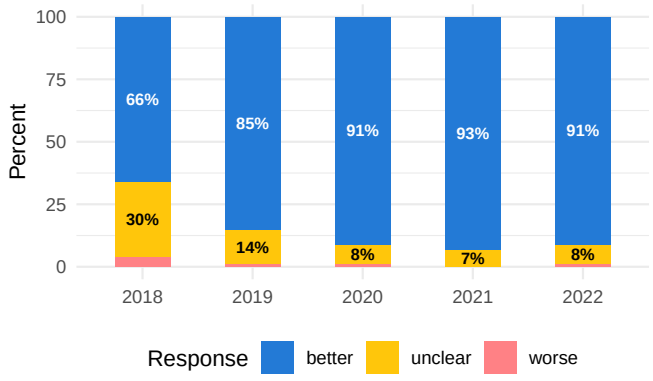
Access and Accuracy (How are Data Accessed, Corrected, Retained, Deleted, and Exported?)

Data Access

6.1.1: Access Data

Do the policies clearly indicate whether or not the company provides authorized individuals a method to access or review a user's personal information?

Figure 71: Access Data



The Access Data evaluation question indicates that there is a process for a user to access or review their information through the product. A company should provide users with the ability to view and access the information and content in their account any time with the product to ensure fair and transparent processing of their data.

Better Practice

Processes to access or review user data are available.

Worse Practice

Processes to access or review user data are not available.

Statutes & Regulations:

- COPPA: (An operator is required to provide a parent or guardian access to review, modify, or delete their children's information or prevent further collection of information.) [327]
- CalOPPA: (If the operator maintains a process for a consumer to review and request changes to any of their personally identifiable information they must provide a description of that process.) [328]
- GDPR: (The controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: ... (b) the existence of the right to request from the controller access to ... personal data ... concerning the data subject.) [329]
- GDPR: (The controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: ... (c) the existence of the right to request from the controller access to ... personal data ... concerning the data subject.) [330]
- GDPR: (The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data.) [331]

[327] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(c); See also 16 C.F.R. Part 312.4(d)(3); 16 C.F.R. Part 312.6.

[328] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(2).

[329] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(2)(b).

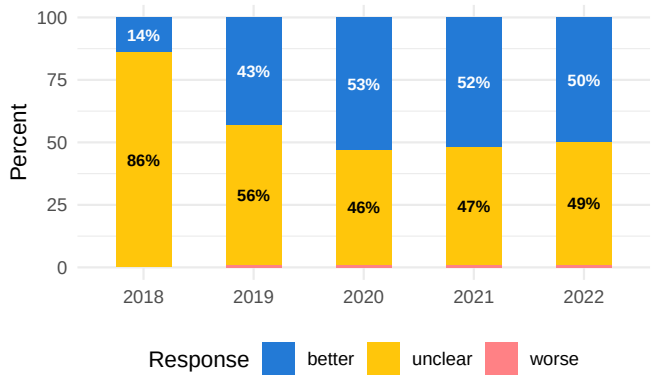
[330] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(c).

[331] General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(1).

6.1.2: Restrict Access

Do the policies clearly indicate whether or not there are methods to restrict what data are accessible to specific users?

Figure 72: Restrict Access



The Restrict Access evaluation question indicates whether processes are available for restricting access to a user's information, or whether mechanisms are used (permissions, roles, or access controls, etc.) to restrict what data is accessible to specific users. A company should respond to a user's request to restrict access to their data if the accuracy of the data is disputed, or the processing is believed to be unlawful, but the user opposes the erasure of their personal data from the product.

Better Practice

Methods are available to restrict who has access to data.

Worse Practice

Methods are not available to restrict who has access to data.

Statutes & Regulations:

- COPPA: (An operator is required to provide a parent or guardian access to review, modify, or delete their children's information or prevent further collection of information.) [332]
- FERPA: (A parent or guardian can request the educational agency to access, modify, or delete their student's education records.) [333]
- GDPR: (The controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: ... (b) the existence of the right to request from the controller ... restriction of processing concerning the data subject.) [334]
- GDPR: (The controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: ... (c) the existence of the right to request from the controller ... restriction of processing concerning the data subject.) [335]
- GDPR: (The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: ... (e) the existence of the right to request from the controller ... restriction of processing concerning the data subject.) [336]

[332] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(c); See also 16 C.F.R. Part 312.4(d)(3); 16 C.F.R. Part 312.6.

[333] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.10; See also 34 C.F.R. Part 99.20.

[334] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(2)(b).

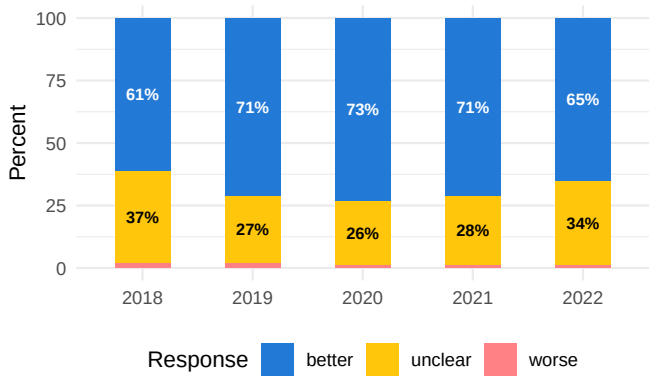
[335] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(c).

[336] General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(1)(e).

6.1.3: Review Data

Do the policies clearly indicate whether or not the company provides a process available for the school, parents, or eligible students to review student information?

Figure 73: Review Data



The Review Data evaluation question indicates whether there is a process for educators in schools, parents at home, or eligible students to review their own personal information or the personal information of their students or children collected by the product. A "better" response to this evaluation question indicates the product does provide a process for educators or parents to review the personal information of their children and students

Better Practice

Processes to review student data are available for the school, parents, or students.

Worse Practice

Processes to review student data are not available for the school, parents, or students.

Statutes & Regulations:

- COPPA: (An operator is required to provide a parent or guardian access to review, modify, or delete their children's information or prevent further collection of information.) [337]
- FERPA: (A parent or guardian can request the educational agency to access, modify, or delete their student's education records.) [338]
- FERPA: (An educational institution is required to use reasonable methods to verify the identity of a parent of a child with whom they disclose information.) [339]
- CalOPPA: (If the operator maintains a process for a consumer to review and request changes to any of their personally identifiable information they must provide a description of that process.) [340]
- AB 1584: (A local educational agency that enters into a contract with a third party must ensure the contract contains a description of the procedures by which a parent, legal guardian, or eligible pupil may review personally identifiable information in the pupil's records and correct erroneous information.) [341]
- CalPPR: (Prohibits schools, school districts, county offices of education, and charter schools from collecting or maintaining information about pupils from social media for any purpose other than school or pupil safety, without notifying each parent or guardian and providing the pupil with access and an opportunity to correct or delete such information.) [342]
- CCPA: ((5) That a consumer has the right to request the specific pieces of personal information the business has collected about that consumer.) [343]
- CCPA: (A business shall, in a form that is reasonably accessible to consumers, make available to consumers two or more designated methods for submitting requests for information, or requests for deletion or correction including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required, or for requests for deletion or correction.) [344]
- CCPA: ("Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, or by a person who has power of attorney or is acting as a conservator for the consumer, and that the business can verify, using commercially reasonable methods to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer to delete personal information, or to correct inaccurate personal information, if the business cannot verify that the consumer making the request is the consumer about whom the business has collected information or is a per-

[337] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(c); See also 16 C.F.R. Part 312.4(d)(3); 16 C.F.R. Part 312.6.
[338] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.10; See also 34 C.F.R. Part 99.20.
[339] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(c).
[340] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(2).
[341] California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(4).
[342] California Privacy of Pupil Records, Cal. Ed. Code § 49073.6(c).
[343] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.110(c)(5).
[344] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.130(a)(1).

son authorized by the consumer to act on such consumer's behalf.)[345]

- CAADCA: (A business shall provide prominent, accessible, and responsive tools to help children, or their parents or guardians, exercise their privacy rights and report concerns.)[346]

[345] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ak).

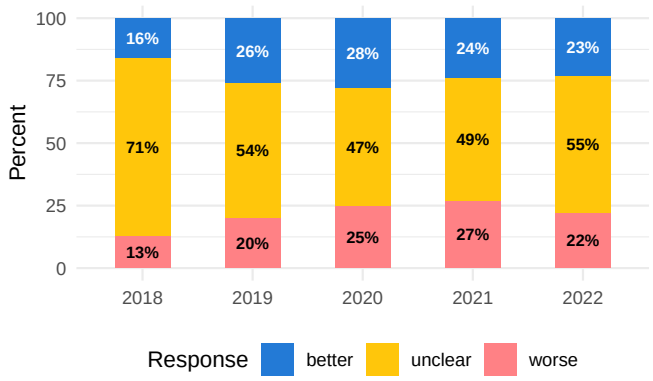
[346] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(a)(10).

Data Integrity

6.2.1: Maintain Accuracy

Do the policies clearly indicate whether or not the company takes steps to maintain the accuracy of data they collect and store?

Figure 74: Maintain Accuracy



The Maintain Accuracy evaluation question indicates whether the company has procedures to keep users' personal information accurate and up to date. A company should respond to a user's request to add, erase, or modify inaccurate personal information.

Better Practice

The company attempts to maintain the accuracy of data they collect.

Worse Practice

The company does not attempt to maintain the accuracy of data they collect.

Statutes & Regulations:

- COPPA: (An operator must take reasonable steps to release a child's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of the information, and provide assurances that they contractually maintain the information in the same manner.) [347]
- COPPA: (An operator must maintain the confidentiality, security, and integrity of personal information collected from children.) [348]
- GDPR: (Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.) [349]
- GDPR: (The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.) [350]

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

[348] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(e); See also 16 C.F.R. Part 312.8.

[349] General Data Protection Regulation (GDPR) 2016/679, Principles relating to processing of personal data, Art. 5(1)(d).

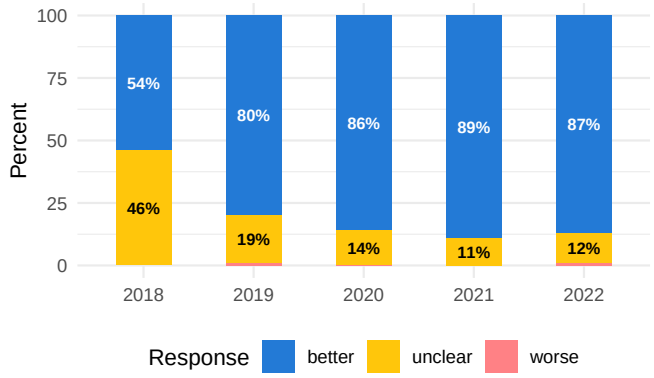
[350] General Data Protection Regulation (GDPR) 2016/679, Right to restriction of processing, Art. 18(1)(a).

Data Correction

6.3.1: Data Modification

Do the policies clearly indicate whether or not the company provides authorized individuals with the ability to modify data?

Figure 75: Data Modification



The Data Modification evaluation question indicates whether there is a process for an authorized user to access and modify information through the product. A company should provide users with the ability to view and edit the information and content in their account, or accounts they manage, to ensure fair and transparent processing of their data.

Better Practice

Processes to modify data are available for authorized users.

Worse Practice

Processes to modify data are not available for authorized users.

Statutes & Regulations:

- CalOPPA: (If the operator maintains a process for a consumer to review and request changes to any of their personally identifiable information they must provide a description of that process.) [351]
- GDPR: (The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.) [352]
- CCPA: (A consumer shall have the right to request a business that maintains inaccurate personal information about the consumer to correct such inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information.) [353]

[351] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(2).

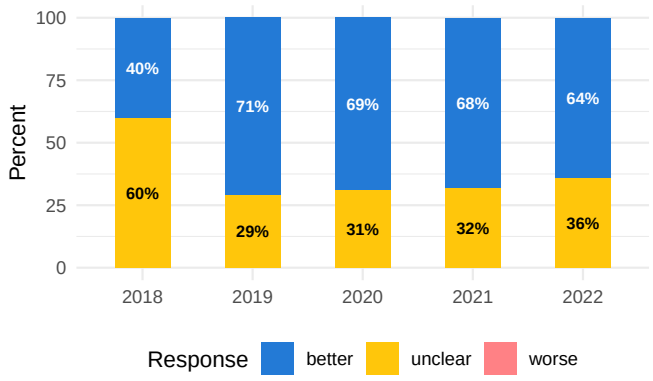
[352] General Data Protection Regulation (GDPR) 2016/679, Right to rectification, Art. 16.

[353] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.106(a).

6.3.2: Modification Process

Do the policies clearly indicate whether or not the company provides a process for the schools, parents, or eligible students to modify inaccurate student information?

Figure 76: Modification Process



The Modification Process evaluation question indicates whether there is a process for educators in schools, parents at home, or eligible students to review their own personal information or the personal information of their students or children collected by the product.

Better Practice

Processes for the school, parents, or students to modify inaccurate student information are available.

Worse Practice

Processes for the school, parents, or students to modify inaccurate student information are not available.

Statutes & Regulations:

- COPPA: (An operator is required to provide a parent or guardian access to review, modify, or delete their children's information or prevent further collection of information.) [354]
- FERPA: (An educational institution is required to use reasonable methods to verify the identity of a parent of a child with whom they disclose information.) [355]
- FERPA: (A parent or guardian can request the educational agency to access, modify, or delete their student's education records.) [356]
- FERPA: (Any rights to access, modify, or delete student records may transfer to an "eligible" student who is over 18 years of age.) [357]
- CalOPPA: (If the operator maintains a process for a consumer to review and request changes to any of their personally identifiable information they must provide a description of that process.) [358]
- AB 1584: (A local educational agency that enters into a contract with a third party must ensure the contract contains a description of the procedures by which a parent, legal guardian, or eligible pupil may review personally identifiable information in the pupil's records and correct erroneous information.) [359]
- CalPPR: (Prohibits schools, school districts, county offices of education, and charter schools from collecting or maintaining information about pupils from social media for any purpose other than school or pupil safety, without notifying each parent or guardian and providing the pupil with access and an opportunity to correct or delete such information.) [360]
- GDPR: (The controller shall communicate any rectification... of personal data ... to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.) [361]
- CCPA: (A business that collects personal information about consumers shall disclose the consumer's right to request correction of inaccurate personal information. A business that receives a verifiable consumer request to correct inaccurate personal information shall use commercially reasonable efforts to correct the inaccurate personal information, as directed by the consumer.) [362]
- CCPA: (A business shall, in a form that is reasonably accessible to consumers, make available to consumers two or more designated methods for submitting requests for information, or requests for deletion or correction including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required, or for requests for deletion or correction.) [363]
- CCPA: ("Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, by a natu-

[354] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(c); See also 16 C.F.R. Part 312.4(d)(3); 16 C.F.R. Part 312.6.
[355] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(c).
[356] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.10; See also 34 C.F.R. Part 99.20.
[357] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.5(a)(1).
[358] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(2).
[359] California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(4).
[360] California Privacy of Pupil Records, Cal. Ed. Code § 49073.6(c).
[361] General Data Protection Regulation (GDPR) 2016/679, Notification obligation regarding rectification or erasure of personal data or restriction of processing, Art. 19.
[362] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.106(b)-(c).
[363] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.130(a)(1).

ral person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, or by a person who has power of attorney or is acting as a conservator for the consumer, and that the business can verify, using commercially reasonable methods to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer to delete personal information, or to correct inaccurate personal information, if the business cannot verify that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.)[364]

- CAADCA: (A business shall provide prominent, accessible, and responsive tools to help children, or their parents or guardians, exercise their privacy rights and report concerns.)[365]

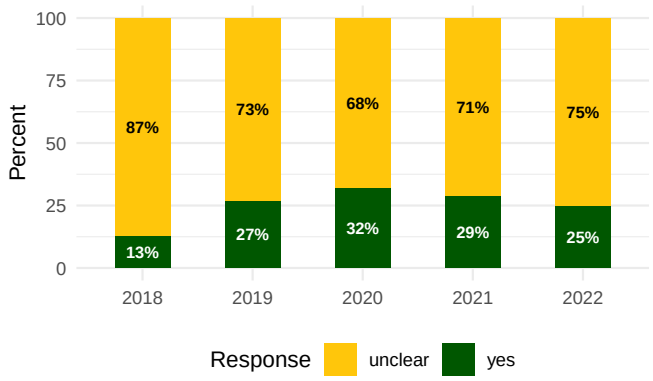
[364] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ak).

[365] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(a)(10).

6.3.3: Modification Time

Do the policies clearly indicate how long the company has to modify a user's inaccurate data after the company is given notice?

Figure 77: Modification Time



The Modification Time evaluation question indicates whether the company provides a time frame in which they will modify a user's information after they have been provided notification of the request from the user.

Transparent Practice

The time period for the company to modify inaccurate data is indicated.

Statutes & Regulations:

- GDPR: (The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.) [366]
- CCPA: (A business shall, in a form that is reasonably accessible to consumers disclose and deliver the required information to a consumer free of charge, or correct inaccurate personal information, or delete a consumer's personal information, based on the consumer's request, within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business's duty to disclose and deliver the information, or correct inaccurate personal information or delete personal information, within 45 days of receipt of the consumer's request. The time period to provide the required information, or to correct inaccurate personal information or delete personal information, may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.) [367]

[366] General Data Protection Regulation (GDPR) 2016/679, Right to rectification, Art. 16.

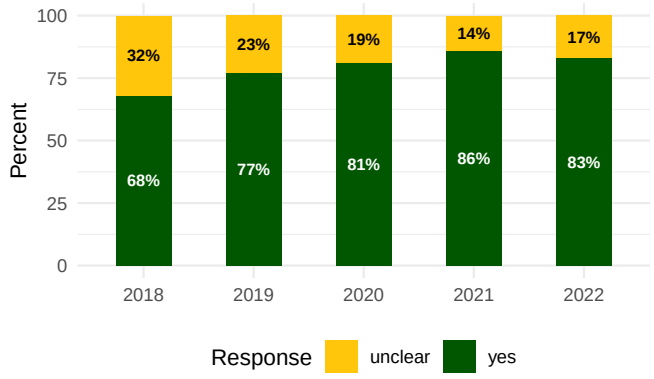
[367] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.130(a)(2)(A).

Data Retention

6.4.1: Retention Policy

Do the policies clearly indicate the company has a data retention policy, including any data sunsets or any time-period after which a user's data will be automatically deleted if they are inactive on the product?

Figure 78: Retention Policy



The Retention Policy evaluation question indicates whether the product has a data retention policy, including any data sunsets or any time period after which a user's data will be automatically deleted if they are inactive on the product. A company should disclose how long different types of data are stored or retained by the company and if different retention periods apply to different users of the product.

Transparent Practice

A data-retention policy is available.

Statutes & Regulations:

- GDPR: (The controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.) [368]
- GDPR: (The controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.) [369]
- GDPR: (The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: ... (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.) [370]
- CCPA: (A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers as to the length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine such period, provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.) [371]
- CAADCA: (A business shall not collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, unless the business can demonstrate a compelling reason that the collecting, selling, sharing, or retaining of the personal information is in the best interests of children.) [372]

[368] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(2)(a).

[369] >General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(a).

[370] General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(1)(d).

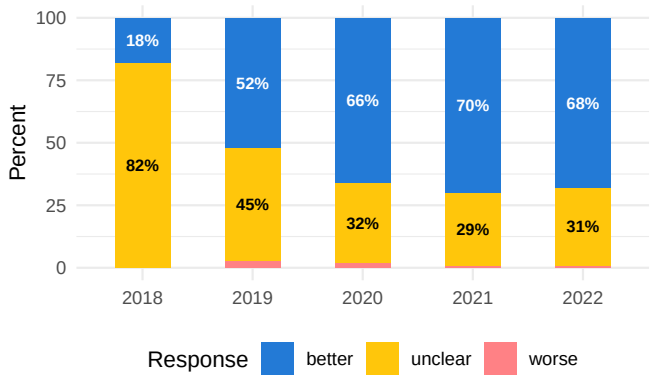
[371] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100(a)(3).

[372] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(b)(3).

6.4.2: Retention Exception

Do the policies clearly indicate whether or not there are any exceptions to the standard data retention policy (including valid requests to inspect the data)?

Figure 79: Retention Exception



The Retention Exception evaluation question indicates whether the retention period for a user's data may be changed for any reason including a legitimate purpose or when an inspection request is received, or other legal investigation request, or to protect the health and safety of other users of the product.

Better Practice

Exceptions to the data retention policy exist.

Worse Practice

Exceptions to the data retention policy do not exist.

Statutes & Regulations:

- FERPA: (An educational institution must annually notify parents of their rights to inspect and review a student's education records, make corrections, delete, or consent to the disclosure of information.) [373]
- GDPR: (Data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.) [374]
- GDPR: (The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: ... (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims.) [375]
- CCPA: (The business may maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws, or for other purposes solely to the extent permissible under this title.) [376]
- CCPA: (A business, or a service provider or contractor, acting pursuant to its contract with the business, another service provider, or another contractor, shall not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the business, service provider, or contractor to maintain the consumer's personal information.) [377]

[373] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.7(a).

[374] General Data Protection Regulation (GDPR) 2016/679, Principles relating to processing of personal data, Art. 5(1)(e).

[375] General Data Protection Regulation (GDPR) 2016/679, Right to restriction of processing, Art. 18(1)(c).

[376] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.105(c)(2).

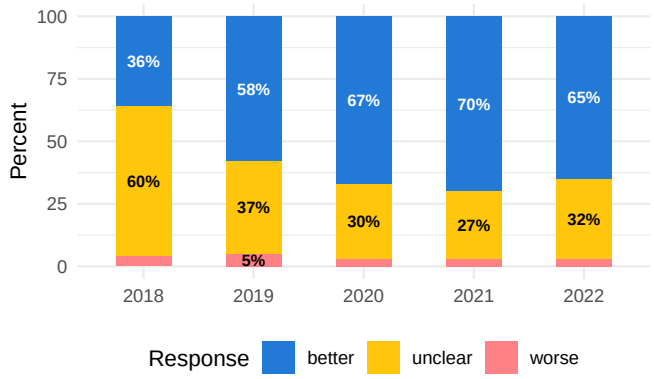
[377] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.105(d)(1)-(8).

Data Deletion

6.5.1: Deletion Purpose

Do the policies clearly indicate whether or not the company will delete a user's personal information when the data are no longer necessary to fulfill its intended purpose?

Figure 80: Deletion Purpose



The Deletion Purpose evaluation question indicates whether a user's data will be deleted when it is no longer necessary for the purpose in which it was collected. A company should delete a user's data after a specified time period in accordance with its retention policy, such as the end of a semester, a period of inactivity on the account, or termination by the user of the user's account.

Better Practice

Data are deleted when no longer necessary.

Worse Practice

Data are not deleted when no longer necessary.

Statutes & Regulations:

- COPPA: (An operator may retain information collected from a child only as long as necessarily to fulfill the purpose for which it was collected and must delete the information using reasonable measures to prevent unauthorized use.) [378]
- AB 1584: (A local educational agency that enters into a contract with a third party must ensure the contract contains a certification that a pupil's records shall not be retained or available to the third party upon completion of the terms of the contract and a description of how that certification will be enforced.) [379]
- GDPR: (The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.) [380]
- CCPA: (A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers as to the length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine such period, provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.) [381]

[378] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.10.

[379] California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(7).

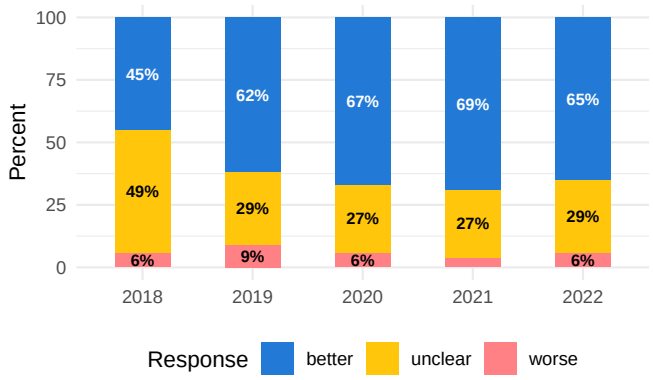
[380] General Data Protection Regulation (GDPR) 2016/679, Right to erasure, Art. 17(1)(a).

[381] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100(a)(3).

6.5.2: Account Deletion

Do the policies clearly indicate whether or not a user's data are deleted upon account cancellation or termination?

Figure 81: Account Deletion



The Account Deletion evaluation question indicates whether a user's data are deleted when their account is canceled or terminated. A company should provide a process for a user to delete their account and all their personal data from the account when the account is canceled or terminated.

Better Practice

A user's data are deleted upon account cancellation or termination.

Worse Practice

A user's data are not deleted upon account cancellation or termination.

Statutes & Regulations:

- COPPA: (An operator may retain information collected from a child only as long as necessarily to fulfill the purpose for which it was collected and must delete the information using reasonable measures to prevent unauthorized use.) [382]
- FERPA: (A parent or guardian can request the educational agency to access, modify, or delete their student's education records.) [383]
- FERPA: (Any rights to access, modify, or delete student records may transfer to an "eligible" student who is over 18 years of age.) [384]
- SOPIPA: (An operator is required to delete personal information at the request of a parent or the school.) [385]
- CCPA: ("Sensitive personal information" means personal information that reveals a consumer's social security, driver's license, state identification card, or passport number; or a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; or a consumer's precise geolocation; or a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; or the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication; or a consumer's genetic data.) [386]

[382] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.10.

[383] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.10; See also 34 C.F.R. Part 99.20.

[384] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.5(a)(1).

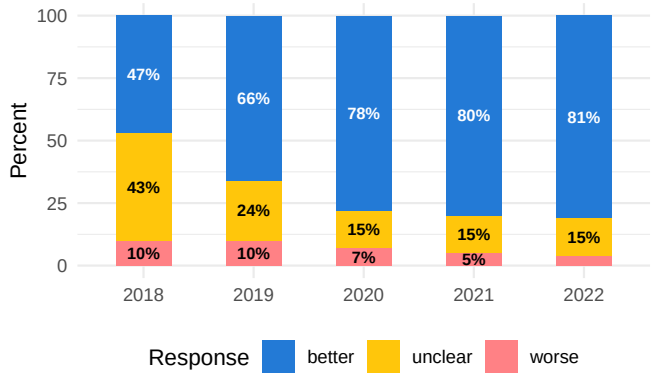
[385] *See* Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(d)(2).

[386] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ae)(1).

6.5.3: User Deletion

Do the policies clearly indicate whether or not a user can delete any of their information from the company?

Figure 82: User Deletion



The User Deletion evaluation question indicates that there is a process for a user to delete their information through the product. A company should provide users with the ability to view and erase the information and content in their account any time with the product to ensure fair and transparent processing of their data.

Better Practice

Processes to delete user data are available.

Worse Practice

Processes to delete user data are not available.

Statutes & Regulations:

- CalOPPA: (If the operator maintains a process for a consumer to review and request changes to any of their personally identifiable information they must provide a description of that process.) [387]
- CalPRMDW: (Prohibits an operator from marketing or advertising non age-appropriate types of products or services to a minor under 18 years of age and from knowingly using, disclosing, compiling, or allowing a third party to use, disclose, or compile, the personal information of a minor for the purpose of marketing or advertising non age-appropriate types of products or services. Also, a minor is permitted to request to "erase" or remove and obtain removal of content or information posted on the operator's site.) [388]
- GDPR: (Where the controller has made the personal data public and is obliged ... to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.) [389]
- CCPA: (A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.) [390]
- GDPR: (The controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: ... (b) the existence of the right to request from the controller ... erasure of personal data ... concerning the data subject.) [391]
- GDPR: (The controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: ... (c) the existence of the right to request from the controller ... erasure of personal data ... concerning the data subject.) [392]
- GDPR: (The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: ... (e) the existence of the right to request from the controller ... erasure of personal data ... concerning the data subject.) [393]
- GDPR: (The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: ... (b) the data subject withdraws consent on which the processing is based ... and where there is no other legal ground for the processing.) [394]
- GDPR: (The controller shall communicate any ... erasure of personal data ... to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.) [395]

[387] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(2).

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

[389] General Data Protection Regulation (GDPR) 2016/679, Right to erasure, Art. 17(2).

[390] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.105(a).

[391] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(2)(b).

[392] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(c).

[393] General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(1)(e).

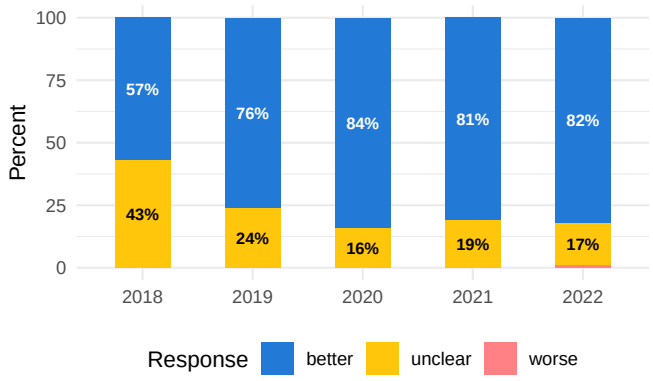
[394] General Data Protection Regulation (GDPR) 2016/679, Right to erasure, Art. 17(1)(b).

[395] General Data Protection Regulation (GDPR) 2016/679, Notification obligation regarding rectification or erasure of personal data or restriction of processing, Art. 19.

6.5.4: Deletion Process

Do the policies clearly indicate whether or not the company provides a process for an authorized user to delete a user's personal information?

Figure 83: Deletion Process



The Deletion Process evaluation question indicates whether there is a process for authorized users including: educators in schools, parents at home, or eligible students to review and delete their own personal information or the personal information of their students or children collected by the product. A company should provide managed account controls or disclose contact information where parents and educators can request to delete data of children or students.

Better Practice

Processes for authorized users to delete data are available.

Worse Practice

Processes for authorized users to to delete data are not available.

Statutes & Regulations:

- COPPA: (An operator is required to provide a parent or guardian access to review, modify, or delete their children's information or prevent further collection of information.) [396]
- FERPA: (A parent or guardian can request the educational agency to access, modify, or delete their student's education records.) [397]
- FERPA: (Any rights to access, modify, or delete student records may transfer to an "eligible" student who is over 18 years of age.) [398]
- SOPIPA: (An operator is required to delete personal information at the request of a parent or the school.) [399]
- CalPPR: (Prohibits schools, school districts, county offices of education, and charter schools from collecting or maintaining information about pupils from social media for any purpose other than school or pupil safety, without notifying each parent or guardian and providing the pupil with access and an opportunity to correct or delete such information.) [400]
- CCPA: (A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. A business that collects personal information about consumers shall disclose the consumer's rights to request the deletion of the consumer's personal information. A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information shall delete the consumer's personal information from its records, notify any service providers or contractors to delete the consumer's personal information from their records, and notify all third parties to whom the business has sold or shared such personal information, to delete the consumer's personal information, unless this proves impossible or involves disproportionate effort.) [401]
- CCPA: (A business shall, in a form that is reasonably accessible to consumers, make available to consumers two or more designated methods for submitting requests for information, or requests for deletion or correction including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required, or for requests for deletion or correction.) [402]
- CCPA: ("Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, or by a person who has power of attorney or is acting as a conservator for the consumer, and that the business can verify, using commercially reasonable methods to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer to delete personal infor-

[396] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(c); See also 16 C.F.R. Part 312.4(d)(3); 16 C.F.R. Part 312.6.
[397] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.10; See also 34 C.F.R. Part 99.20.
[398] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.5(a)(1).
[399] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(d)(2).
[400] California Privacy of Pupil Records, Cal. Ed. Code § 49073.6(c).
[401] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.105(a)-(c)(1)-(3).
[402] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.130(a)(1).

mation, or to correct inaccurate personal information, if the business cannot verify that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.)[403]

- CAADCA: (A business shall provide prominent, accessible, and responsive tools to help children, or their parents or guardians, exercise their privacy rights and report concerns.)[404]

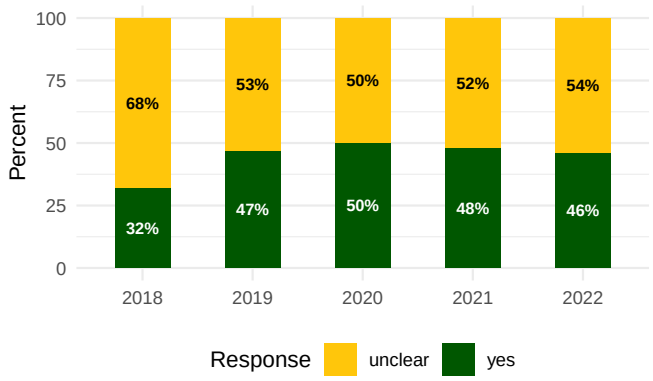
[403] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ak).

[404] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(a)(10).

6.5.5: Deletion Time

Do the policies clearly indicate how long the company may take to delete a user's data after the company is given notice?

Figure 84: Deletion Time



The Deletion Time evaluation question indicates whether the company provides a time frame in which they will delete a user's information from the product after they have been provided notification of the request from the user.

Transparent Practice

The time period for the company to delete data is indicated.

Statutes & Regulations:

- GDPR: (The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.) [405]
- GDPR: (The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay ...) [406]
- CCPA: (A business shall, in a form that is reasonably accessible to consumers disclose and deliver the required information to a consumer free of charge, or correct inaccurate personal information, or delete a consumer's personal information, based on the consumer's request, within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business's duty to disclose and deliver the information, or correct inaccurate personal information or delete personal information, within 45 days of receipt of the consumer's request. The time period to provide the required information, or to correct inaccurate personal information or delete personal information, may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.) [407]

[405] General Data Protection Regulation (GDPR) 2016/679, Right to rectification, Art. 16.

[406] General Data Protection Regulation (GDPR) 2016/679, Right to erasure, Art. 17(1).

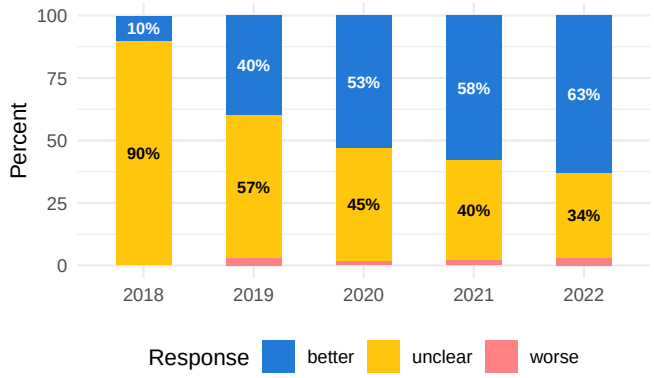
[407] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.130(a)(2)(A).

Data Portability

6.6.1: User Export

Do the policies clearly indicate whether or not a user can export or download their data, including any user created content on the product?

Figure 85: User Export



The User Export evaluation question indicates whether a user can export or download their data from the product, including any user-created content on the product in a structured data format for use with another product. A company should provide a process for a user to export or download their data from the product.

Better Practice

Processes to download user data are available.

Worse Practice

Processes to download user data are not available.

Statutes & Regulations:

- SOPIPA: (An operator is required to allow a student or parent to export, save, or maintain their own student created data or content.) [408]
- AB 1584: (A local educational agency that enters into a contract with a third party must ensure the contract contains a description of the means by which pupils may retain possession and control of their own pupil-generated content, including options by which a pupil may transfer pupil-generated content to a personal account.) [409]
- GDPR: (The controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: ... (b) the existence of the right to ... data portability.) [410]
- GDPR: (The controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: ... (c) the existence of the right to ... data portability.) [411]
- GDPR: (The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.) [412]
- GDPR: (In exercising his or her right to data portability ... the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.) [413]
- CCPA: (A business shall, in a form that is reasonably accessible to consumers disclose and deliver the required information to a consumer free of charge, or correct inaccurate personal information, or delete a consumer's personal information, based on the consumer's request, within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business's duty to disclose and deliver the information, or correct inaccurate personal information or delete personal information, within 45 days of receipt of the consumer's request. The time period to provide the required information, or to correct inaccurate personal information or delete personal information, may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.) [414]
- GDPR: (The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.) [415]

[408] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(r).

[409] California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(2).

[410] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(2)(b).

[411] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(c).

[412] General Data Protection Regulation (GDPR) 2016/679, Right to data portability, Art. 20(1).

[413] General Data Protection Regulation (GDPR) 2016/679, Right to data portability, Art. 20(2).

[414] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.130(a)(2)(A).

[415] General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(3).

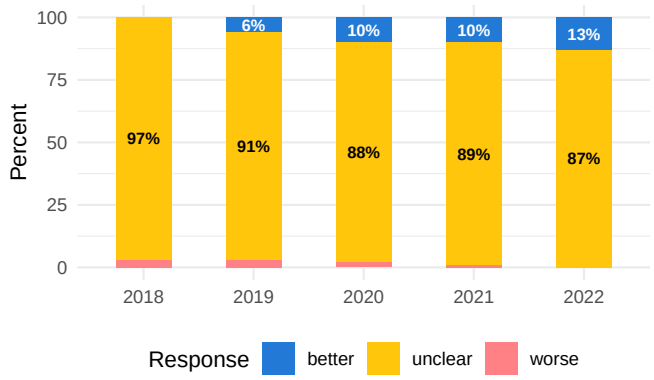
- CCPA: (A business shall, in a form that is reasonably accessible to consumers provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format, which also may be transmitted to another entity at the consumer's request without hindrance. “Specific pieces of information” do not include data generated to help ensure security and integrity or as prescribed by regulation. Personal information is not considered to have been disclosed by a business when a consumer instructs a business to transfer the consumer's personal information from one business to another in the context of switching services.) [416]

[416] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.130(a)(3)(B)(iii).

6.6.2: Legacy Contact

Do the policies clearly indicate whether or not a user may assign an authorized user or legacy contact to access and download their data?

Figure 86: Legacy Contact



The Legacy Contact evaluation question indicates that the product provides a process to assign a managed account owner or authorized trusted contact if the account becomes inactive in order to retain access to the user's information and content in the event of the user's impairment or death. A company should provide a process to assign a managed account owner or authorized trusted contact for the purposes of digital inheritance.

Better Practice

A user can assign an authorized account manager or legacy contact.

Worse Practice

A user can not assign an authorized account manager or legacy contact.

Statutes & Regulations:

- RUFADAA: (Authorizes a decedent's personal representative or trustee to access and manage their digital assets and electronic communications stored with an online service provider, and give directions regarding the disclosure of those assets.) [417]

[417] California Revised Uniform Fiduciary Access to Digital Assets Act, Cal. Prob. Code § 870-884.

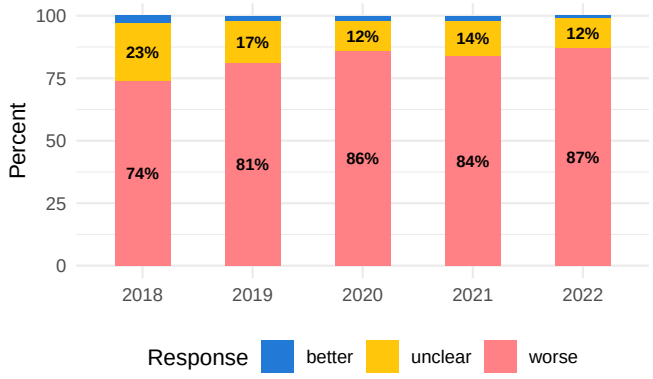
Data Transfer (How are Data Transferred During a Bankruptcy, Merger, or Acquisition?)

Data Handling

7.1.1: Transfer Data

Do the policies clearly indicate whether or not the company can transfer a user's data in the event of the company's merger, acquisition, or bankruptcy?

Figure 87: Transfer Data



The Transfer Data evaluation question indicates whether a user's information may be transferred as an asset to a successor third party in the event of a merger, acquisition, or bankruptcy. A company should carefully consider whether to transfer a user's personal information to a third party in exchange for monetary value because of the increased risk the personal information may be used for unintended purposes.

Better Practice

User information cannot be transferred to a third party in the event of a merge, acquisition, or bankruptcy.

Worse Practice

User information can be transferred to a third party in the event of a merge, acquisition, or bankruptcy.

Statutes & Regulations:

- COPPA: (Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.) [418]
- SOPIPA: (An operator may transfer a student's personal information to a third party in the event of a merger, acquisition, or bankruptcy, but the successor entity is subject to the same onward data privacy and security obligations.) [419]
- CCPA: (A business does not sell personal information when the business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title.) [420]

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

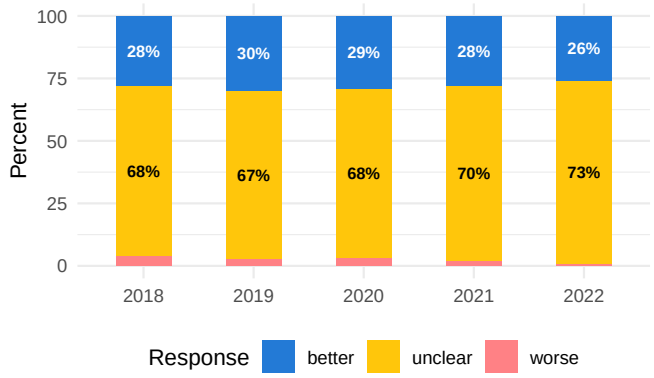
[419] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(3).

[420] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ad)(2)(C).

7.1.2: Transfer Notice

Do the policies clearly indicate whether or not the company will notify users of a data transfer to a third-party successor, in the event of a company's bankruptcy, merger, or acquisition?

Figure 88: Transfer Notice



The Transfer Notice evaluation question indicates whether users may delete their data before it is transferred as an asset to a successor third party in the event of a merger, acquisition, or bankruptcy. A company should provide the ability for users to delete their data in the event their personal information may be transferred to a third party to allow each user to make an informed decision whether or not to continue using the product.

Better Practice

Users are notified if their information is transferred to a third party.

Worse Practice

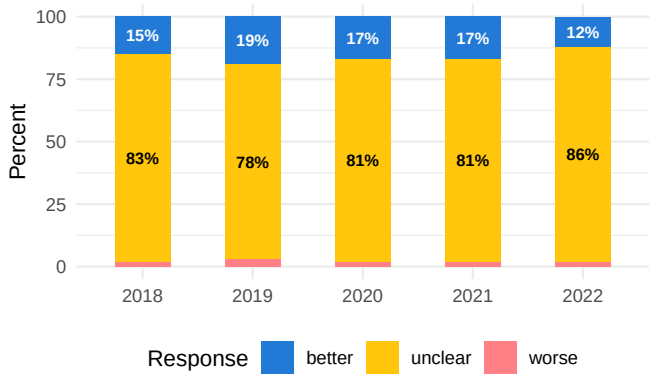
Users are not notified if their information is transferred to a third party.

Transfer Request

7.2.1: Transfer Deletion

Do the policies clearly indicate whether or not a user can request to delete their data prior to its transfer to a third-party successor in the event of a company bankruptcy, merger, or acquisition?

Figure 89: Transfer Deletion



The Transfer Deletion evaluation question indicates whether notice is provided to users that they may delete their data before a user's information is transferred as an asset to a successor third party in the event of a merger, acquisition, or bankruptcy. A company should provide notice and allow users to delete their data as a best practice in the event their personal information is transferred to a third party to allow the user to make an informed decision whether or not to continue using the product.

Better Practice

User information can be deleted prior to its transfer to a third party.

Worse Practice

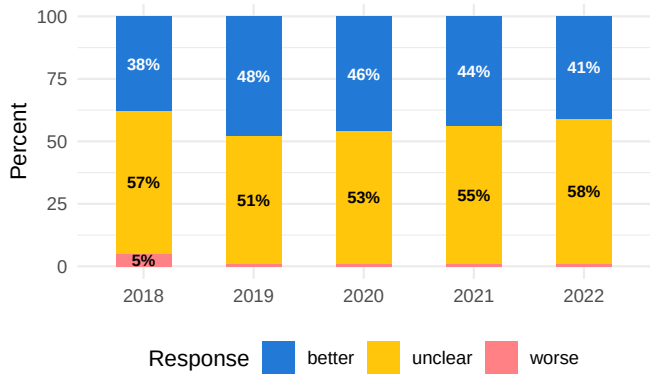
User information can not be deleted prior to its transfer to a third party.

Onward Contractual Obligations

7.3.1: Transfer Limits

Do the policies clearly indicate whether or not the third-party successor of a data transfer is contractually required to provide the same privacy compliance required of the company?

Figure 90: Transfer Limits



The Transfer Limits evaluation question indicates whether the company places contractual obligations or restrictions on the use of users' data on the successor third party in the event of a merger, acquisition, or bankruptcy. A successor third party should adopt the company's privacy policies for the product and process data in accordance with the same privacy practices that users provided their informed consent in order to prevent users' personal information from being used for unintended purposes.

Better Practice

Third-party transfer is contractually required to use the same privacy practices.

Worse Practice

Third-party transfer is not contractually required to use the same privacy practices.

Statutes & Regulations:

- COPPA: (An operator must take reasonable steps to release a child's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of the information, and provide assurances that they contractually maintain the information in the same manner.)[421]
- SOPIPA: (An operator may transfer a student's personal information to a third party in the event of a merger, acquisition, or bankruptcy, but the successor entity is subject to the same onward data privacy and security obligations.)[422]
- GDPR: (Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.)[423]

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

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

[423] General Data Protection Regulation (GDPR) 2016/679, General principle for transfers, Art. 44.

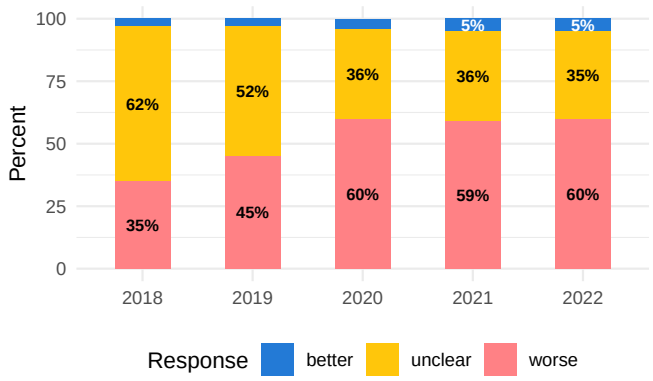
Security (How are Data Transmitted, Stored, and Protected?)

User Identity

8.1.1: Verify Identity

Do the policies clearly indicate whether or not the company or an authorized third party verifies a user's identity with additional personal information?

Figure 91: Verify Identity



The Verify Identity evaluation question indicates that additional personal information is collected from a user by the product to verify their identity with a government-issued identification or with other forms of identification that could be connected to their offline identity. A company should not require users to provide sensitive information about their offline identity unless necessary to protect the personal information of the user for which the request to access, modify, delete, or export their personal information and requires the extra security of verifying their identity.

Better Practice

A user's identity is not verified with additional personal information.

Worse Practice

A user's identity is verified with additional personal information.

Statutes & Regulations:

- FERPA: (An educational institution is required to use reasonable methods to verify the identity of a parent of a child with whom they disclose information.)[424]
- COPPA: (An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology and existing methods available to a parent to prove their identity.)[425]
- GDPR: (The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.)[426]
- GDPR: (Where the controller has reasonable doubts concerning the identity of the natural person making the request ... the controller may request the provision of additional information necessary to confirm the identity of the data subject.)[427]
- CCPA: (A business shall, in a form that is reasonably accessible to consumers use any personal information collected from the consumer in connection with the business's verification of the consumer's request solely for the purposes of verification, and shall not further disclose the personal information, retain it longer than necessary for purposes of verification, or use it for unrelated purposes.)[428]
- CCPA: ("Sensitive personal information" means personal information that reveals a consumer's social security, driver's license, state identification card, or passport number; or a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; or a consumer's precise geolocation; or a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; or the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication; or a consumer's genetic data.)[429]

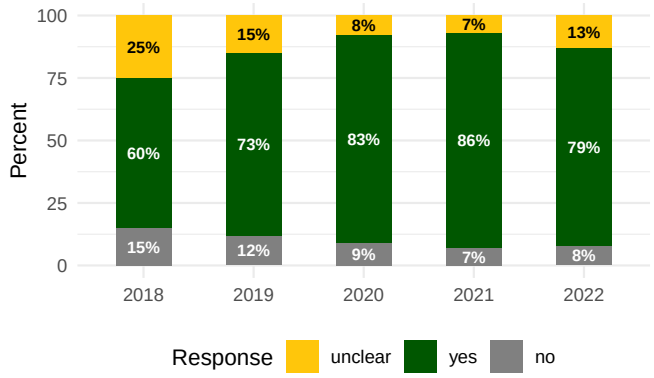
[424] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(c).
[425] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(b)(i)-(iv).
[426] General Data Protection Regulation (GDPR) 2016/679, Conditions Applicable to Child's Consent in Relation to Information Society Services, Art. 8(2).
[427] General Data Protection Regulation (GDPR) 2016/679, Transparent information, communication and modalities for the exercise of the rights of the data subject, Art. 12(6).
[428] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.130(a)(7).
[429] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ae)(1).

User Account

8.2.1: Account Required

Do the policies indicate whether or not the company requires a user to create an account with a username and password in order to use the product?

Figure 92: Account Required



The Account Required evaluation question indicates whether the product allows users to create an account to protect their personal information. A product should allow users to create an account and authenticate it in order to provide user controls to access, edit, delete, and export their information as well as settings to control how their data is used.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

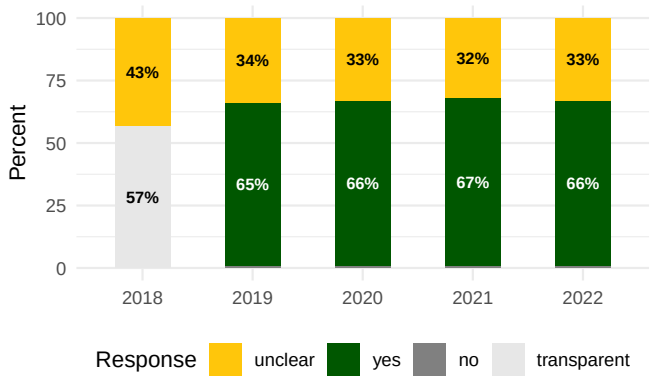
- CCPA: (The disclosure of the required information shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request, provided that if the consumer has an account with the business, the business may require the consumer to use that account to submit a verifiable consumer request.) [430]

[430] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.130(a)(2)(A).

8.2.2: Managed Account

Do the policies clearly indicate whether or not the company provides user managed accounts for other authorized users (eg. a parent, teacher, school or district)?

Figure 93: Managed Account



The Managed Account evaluation question indicates whether managed accounts or parental controls are available for parents, teachers, schools or districts to access, review, edit, and delete the personal information of children or students. A company should create a managed account or child profile if the intended audience of the product includes children or students, because it allows the product to provide better privacy-protecting data collection and use practices to users who use the managed account or profile.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

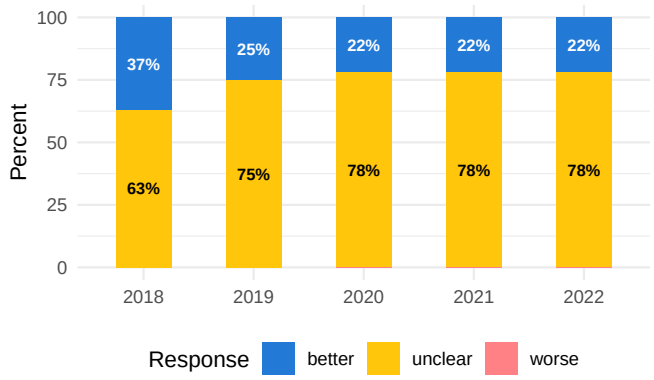
- CAADCA: (If the online service, product, or feature allows the child's parent, guardian, or any other consumer to monitor the child's online activity or track the child's location, the business must provide an obvious signal to the child when the child is being monitored or tracked.)[431]

[431] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(a)(8).

8.2.3: Multi-Factor Protection

Do the policies clearly indicate whether or not the security of a user's account is protected by multi-factor authentication?

Figure 94: Multi-Factor Protection



The Multi-Factor Protection evaluation question indicates whether user accounts can be protected with additional multi-factor authentication for better security through the use of mobile SMS or a third-party authenticator service.

Better Practice

Multi-factor account protection is available.

Worse Practice

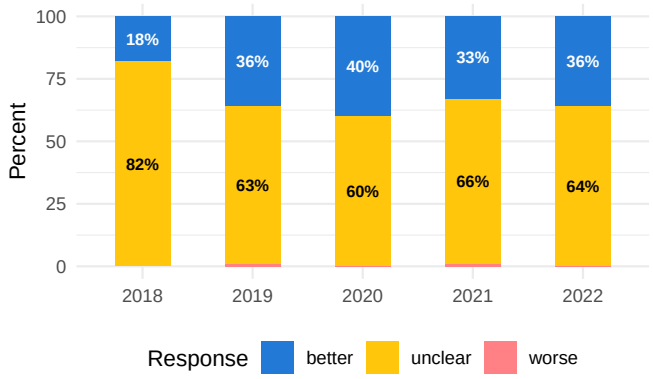
Multi-factor account protection is not available.

Third-Party Security

8.3.1: Security Agreement

Do the policies clearly indicate whether or not a third party with access to a user's information is contractually required to provide the same level of security protections as the company?

Figure 95: Security Agreement



The Security Agreement evaluation question indicates whether contractual obligations are imposed on third-party service providers to require additional security protections for users' personal information. A company should put in place contractual obligations that require third parties to use the same security practices as the product in accordance with the company's privacy policy. Without contractual requirements on third-party security practices of data collected from children and students, parents and educators cannot reasonably expect that the privacy provisions outlined in the product's policies will be honored by third parties that have access to personal data.

Better Practice

Third-parties with access to information are required to provide the same security protections as the company.

Worse Practice

Third-parties with access to information are not required to provide the same security protections as the company.

Statutes & Regulations:

- COPPA: (An operator must take reasonable steps to release a child's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of the information, and provide assurances that they contractually maintain the information in the same manner.) [432]
- FERPA: (An educational institution must maintain physical, technical, and administrative safeguards to protect student information.) [433]
- SOPIPA: (A third party service provider must maintain reasonable security procedures and practices.) [434]
- AB 1584: (A local educational agency that enters into a contract with a third party must ensure the contract contains a description of the actions the third party will take, including the designation and training of responsible individuals, to ensure the security and confidentiality of pupil records.) [435]
- GDPR: (Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.) [436]
- GDPR: (The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller.) [437]

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

[433] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(ii).

[434] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4)(E)(iii)

[435] California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(5).

[436] *See* General Data Protection Regulation (GDPR) 2016/679, Processor, Art. 28(1).

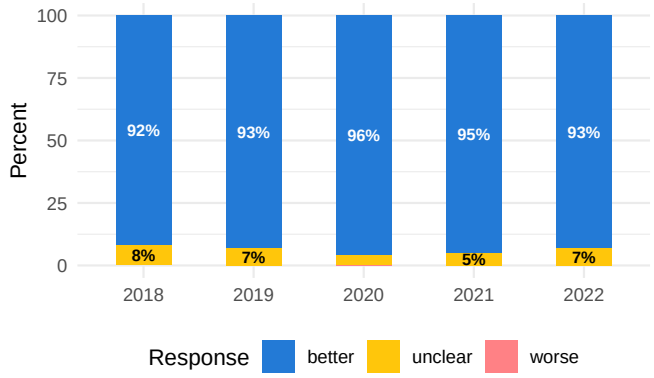
[437] *See* General Data Protection Regulation (GDPR) 2016/679, Security of processing, Art. 32(4).

Data Confidentiality

8.4.1: Reasonable Security

Do the policies clearly indicate whether or not reasonable security standards are used to protect the confidentiality of a user's personal information?

Figure 96: Reasonable Security



The Reasonable Security evaluation question indicates whether any security protections are in place with the product for users' information based on industry standards and best practices. A company should use various technologies and security processes that are continuously updated to protect users' personal information collected by the product from unauthorized access.

Better Practice

Reasonable security practices are used to protect data.

Worse Practice

Reasonable security practices are not used to protect data.

Statutes & Regulations:

- COPPA: (An operator must maintain the confidentiality, security, and integrity of personal information collected from children.) [438]
- DataBreach: (A person or business that owns, licenses, or maintains personal information about a California resident is required to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.) [439]
- COPPA: (An operator must take reasonable steps to release a child's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of the information, and provide assurances that they contractually maintain the information in the same manner.) [440]
- SOPIPA: (An operator is required to implement reasonable security procedures, practices, and protect student data from unauthorized access, destruction, use, modification, or disclosure.) [441]
- FERPA: (An educational institution must maintain physical, technical, and administrative safeguards to protect student information.) [442]
- AB 1584: (A local educational agency that enters into a contract with a third party must ensure the contract contains a description of the actions the third party will take, including the designation and training of responsible individuals, to ensure the security and confidentiality of pupil records.) [443]
- GDPR: (Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.) [444]
- GDPR: (Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: ...(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.) [445]
- GDPR: (In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.) [446]
- CCPA: (A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal

[438] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(e); See also 16 C.F.R. Part 312.8.

[439] California Data Breach Notification Requirements, Cal. Civ. Code § 1798.81.5.

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

[441] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(d)(1).

[442] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(ii).

[443] California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(5).

[444] General Data Protection Regulation (GDPR) 2016/679, Principles relating to processing of personal data, Art. 5(1)(f).

[445] General Data Protection Regulation (GDPR) 2016/679, Security of processing, Art. 32(1)(b).

[446] General Data Protection Regulation (GDPR) 2016/679, Security of processing, Art. 32(2).

access, destruction, use, modification, or disclosure.)[447]

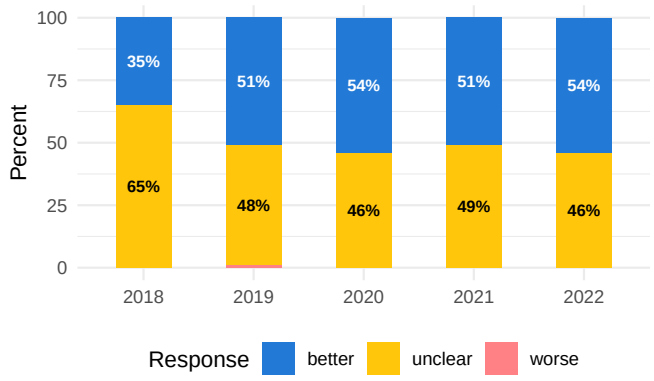
- CCPA: ("Security and Integrity" means the ability of a network or an information system to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information; to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions, and to help prosecute those responsible for such actions; and a business to ensure the physical safety of natural persons.)[448]

[447] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100(e).
[448] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ac).

8.4.2: Physical Access

Do the policies clearly indicate whether or not the company implements physical access controls or limits employee access to user information?

Figure 97: Physical Access



The Physical Access evaluation question indicates that the company implements physical access controls or limits employee access to user information only on a need-to-know basis to better protect users from unauthorized access of their data for unintended purposes.

Better Practice

Employee or physical access to user information is limited.

Worse Practice

Employee or physical access to user information is not limited.

Statutes & Regulations:

- AB 1584: (A local educational agency that enters into a contract with a third party must ensure the contract contains a description of the actions the third party will take, including the designation and training of responsible individuals, to ensure the security and confidentiality of pupil records.) [449]
- CCPA: (A business shall ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements and how to direct consumers to exercise their rights.) [450]

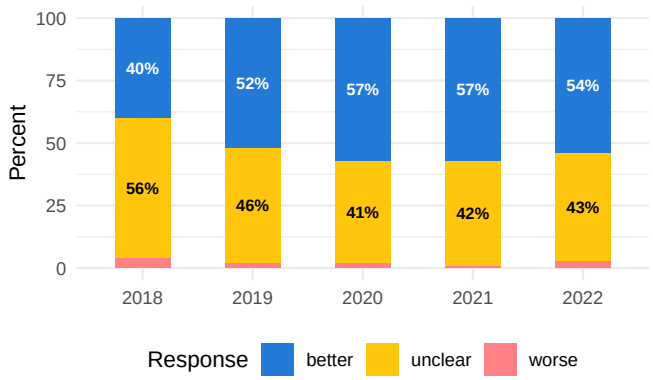
[449] California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(5).
[450] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.135(c)(3).

Data Transmission

8.5.1: Transit Encryption

Do the policies clearly indicate whether or not all data in transit is encrypted?

Figure 98: Transit Encryption



The Transit Encryption evaluation question indicates that a user's personal information collected by the product is transmitted in an encrypted format such as Transport Layer Security (TLS). A company should not collect and transmit personal information over the internet without encryption because the personal information could be intercepted by unauthorized individuals which increases the risk a user's data is used for unintended purposes.

Better Practice

All data in transit are encrypted.

Worse Practice

All data in transit are not encrypted.

Statutes & Regulations:

- DataBreach: (A person or business that owns, licenses, or maintains personal information about a California resident is required to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.) [451]
- GDPR: (Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data.) [452]
- CCPA: (Any consumer whose nonencrypted and nonredacted personal information, or whose email address in combination with a password or security question and answer that would permit access to the account, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action.) [453]

[451] California Data Breach Notification Requirements, Cal. Civ. Code § 1798.81.5.

[452] General Data Protection Regulation (GDPR) 2016/679, Security of processing, Art. 32(1)(a).

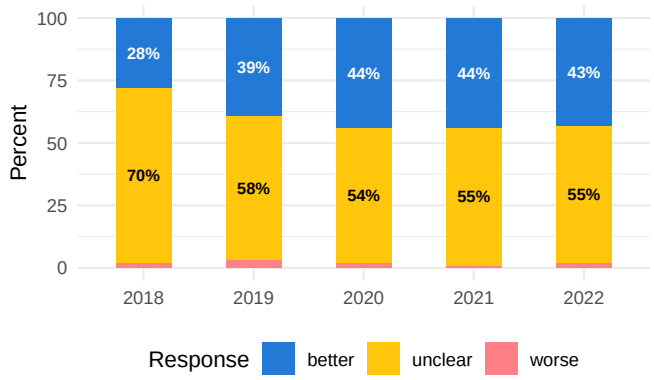
[453] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1)-(2).

Data Storage

8.6.1: Storage Encryption

Do the policies clearly indicate whether or not all data in storage is encrypted?

Figure 99: Storage Encryption



The Storage Encryption evaluation question indicates that a user's data is stored in the company's data servers in an encrypted format. A company should not collect and store a user's personal information without encryption because the personal information could be accessed by unauthorized individuals or disclosed in a data breach, which increases the risk that a user's data is used for unintended purposes.

Better Practice

All data are stored in an encrypted format.

Worse Practice

All data are not stored in an encrypted format.

Statutes & Regulations:

- DataBreach: (A person or business that owns, licenses, or maintains personal information about a California resident is required to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.)[454]
- GDPR: (Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data.)[455]
- CCPA: (Any consumer whose nonencrypted and nonredacted personal information, or whose email address in combination with a password or security question and answer that would permit access to the account, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action.)[456]

[454] California Data Breach Notification Requirements, Cal. Civ. Code § 1798.81.5.

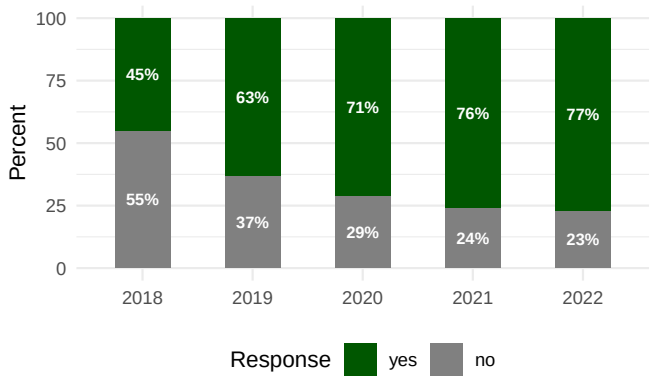
[455] General Data Protection Regulation (GDPR) 2016/679, Security of processing, Art. 32(1)(a).

[456] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1)-(2).

8.6.2: Data Jurisdiction

Do the policies clearly indicate what jurisdiction a user's personal information may be subject to?

Figure 100: Data Jurisdiction



The Data Jurisdiction evaluation question indicates what jurisdiction a user's personal information is or may be subject to. A company should maintain its users' data in its home jurisdiction because other countries may have privacy and data protection laws that are potentially more or less protective than the laws of the country where a user's data is stored.

Transparent Practice

The company is clear what jurisdiction a user's personal information is subject to.

Statutes & Regulations:

- COPPA: (An operator must maintain the confidentiality, security, and integrity of personal information collected from children.) [457]
- COPPA: (An operator must take reasonable steps to release a child's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of the information, and provide assurances that they contractually maintain the information in the same manner.) [458]
- SOPIPA: (A third party service provider must maintain reasonable security procedures and practices.) [459]
- AB 1584: (A local educational agency that enters into a contract with a third party must ensure the contract contains a statement that pupil records continue to be the property of and under the control of the local educational agency.) [460]
- GDPR: (Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: ... (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.) [461]
- GDPR: (Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.) [462]

[457] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(e); See also 16 C.F.R. Part 312.8.

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

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

[460] *See* California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(1).

[461] *See* General Data Protection Regulation (GDPR) 2016/679, Security of processing, Art. 32(1)(c).

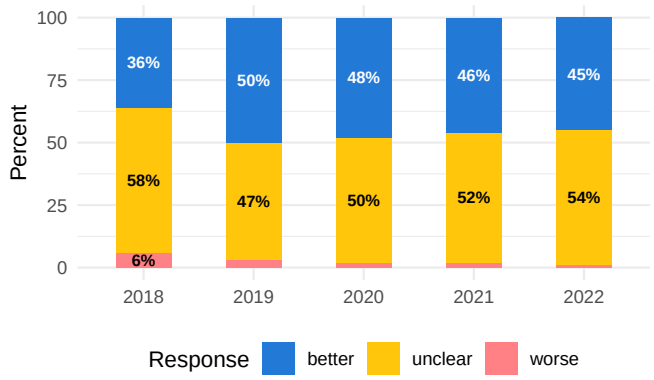
[462] General Data Protection Regulation (GDPR) 2016/679, General principle for transfers, Art. 44.

Data Breach

8.7.1: Breach Notice

Do the policies clearly indicate whether or not the company provides notice in the event of a data breach?

Figure 101: Breach Notice



The Breach Notice evaluation question indicates that in the event of a data breach, the company will provide notice to any users affected. A company should provide notice to users in the event their data is disclosed in a data breach because there is an increased risk the data may be used for unintended purposes.

Better Practice

Notice is provided in the event of a data breach.

Worse Practice

Notice is not provided in the event of a data breach.

Statutes & Regulations:

- DataBreach: (A business that collects personal information from California consumers is required to disclose a breach of the security of their system following discovery or notification of the breach in the security of a consumer's data whose unencrypted personal information was reasonably believed to have been acquired by an unauthorized person.)[463]
- AB 1584: (A local educational agency that enters into a contract with a third party must ensure the contract contains a description of the procedures for notifying the affected parent, legal guardian, or eligible pupil in the event of an unauthorized disclosure of the pupil's records.)[464]
- GDPR: ("personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.)[465]
- GDPR: (In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.)[466]
- GDPR: (The processor shall notify the controller without undue delay after becoming aware of a personal data breach.)[467]
- GDPR: (The notification ... shall at least: (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.)[468]
- GDPR: (Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.)[469]
- GDPR: (The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.)[470]
- GDPR: (When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.)[471]

[463] California Data Breach Notification Requirements, Cal. Civ. Code § 1798.29; § 1798.29(h)(4); § 1798.82.

[464] California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(6).

[465] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(12).

[466] General Data Protection Regulation (GDPR) 2016/679, Notification of a personal data breach to the supervisory authority, Art. 33(1).

[467] General Data Protection Regulation (GDPR) 2016/679, Notification of a personal data breach to the supervisory authority, Art. 33(2).

[468] General Data Protection Regulation (GDPR) 2016/679, Notification of a personal data breach to the supervisory authority, Art. 33(3)(a)-(d).

[469] General Data Protection Regulation (GDPR) 2016/679, Notification of a personal data breach to the supervisory authority, Art. 33(4).

[470] General Data Protection Regulation (GDPR) 2016/679, Notification of a personal data breach to the supervisory authority, Art. 33(5).

[471] General Data Protection Regulation (GDPR) 2016/679, Communication of a personal data breach to the data subject, Art. 34(1).

- GDPR: (Communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and the recommendations provided.) [472]
- GDPR: (The communication to the data subject ... shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects ... is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.) [473]
- CCPA: (Any consumer whose nonencrypted and nonredacted personal information, or whose email address in combination with a password or security question and answer that would permit access to the account, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action.) [474]

[472] General Data Protection Regulation (GDPR) 2016/679, Communication of a personal data breach to the data subject, Art. 34(2).

[473] General Data Protection Regulation (GDPR) 2016/679, Communication of a personal data breach to the data subject, Art. 34(3)(a)-(c).

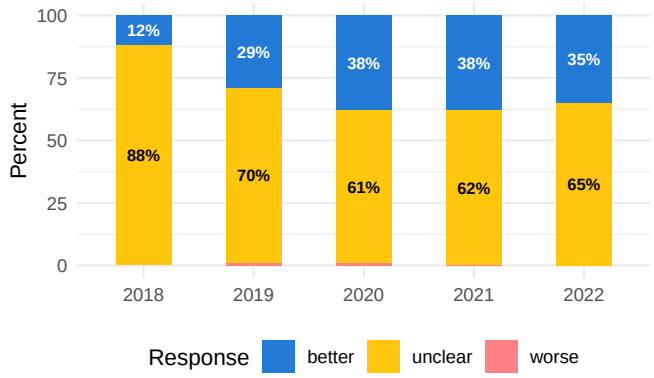
[474] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a)(1)-(2).

Data Oversight

8.8.1: Audit Practices

Do the policies clearly indicate whether or not the data privacy or security practices of the company are internally or externally audited?

Figure 102: Audit Practices



The Audit Practices evaluation question indicates whether the company has internal or external privacy or security staff assessments or audits to ensure user data is secure. A company should implement occasional privacy and security assessments that are continuously updated to protect users' personal information collected by the product from unauthorized access.

Better Practice

Data-privacy and/or security-compliance audits are performed.

Worse Practice

Data-privacy and/or security-compliance audits are not performed.

Statutes & Regulations:

- GDPR: (The controller shall be responsible for, and be able to demonstrate compliance with ... processing of personal data.)[475]
- GDPR: (Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.)[476]
- GDPR: (Where proportionate in relation to processing activities, the responsibility of the controller ... shall include the implementation of appropriate data protection policies by the controller.)[477]
- GDPR: (Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: ... (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.)[478]
- CAADCA: (The term "Data Protection Impact Assessment" means a systematic survey to assess and mitigate risks that arise from the data management practices of the business to children who are reasonably likely to access the online service, product, or feature at issue that arises from the provision of that online service, product, or feature.)[479]
- CAADCA: (A business shall before any new online services, products, or features are offered to the public, complete a Data Protection Impact Assessment for any online service, product, or feature likely to be accessed by children and maintain documentation of this assessment as long as the online service, product, or feature is likely to be accessed by children.)[480]

[475] General Data Protection Regulation (GDPR) 2016/679, Principles relating to processing of personal data, Art. 5(2).

[476] General Data Protection Regulation (GDPR) 2016/679, Responsibility of the controller, Art. 24(1).

[477] General Data Protection Regulation (GDPR) 2016/679, Responsibility of the controller, Art. 24(2).

[478] General Data Protection Regulation (GDPR) 2016/679, Security of processing, Art. 32(1)(d).

[479] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.30(b)(2).

[480] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(a)(1)(A)-(B),(2)-(4),(c).

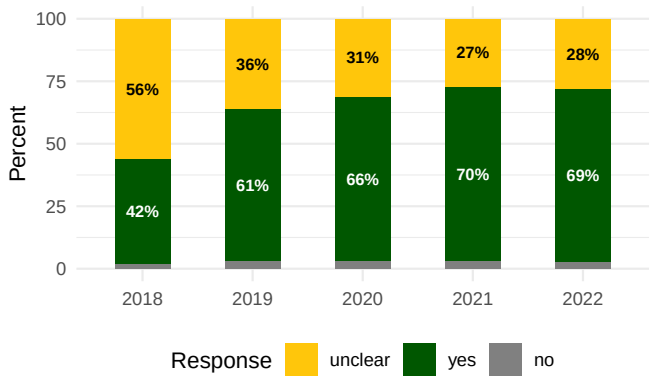
Responsible Use (How are Social Interactions Managed and User Information Displayed?)

Social Interactions

9.1.1: Safe Interactions

Do the policies clearly indicate whether or not a user can interact with trusted users?

Figure 103: Safe Interactions



The Safe Interactions evaluation question indicates whether users can have social interactions with trusted or other known users, such as with students in the same classroom or school, or friends they know in real life. A company should only provide safe interactions for children and students with users that they already know or have a real-life relationship with offline to prevent inappropriate conversations with adults that could cause social, emotional, or physical harm.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

- COPPA: (An operator is required to disclose whether the service enables a child to make personal information publicly available.) [481]
- COPPA: (An operator is prohibited from making personal information from a child publicly available in identifiable form by any means, including a public posting through the Internet, or through a personal home page or screen posted on a Web site or online service, a pen pal service, an electronic mail service, a message board, or a chat room.) [482]

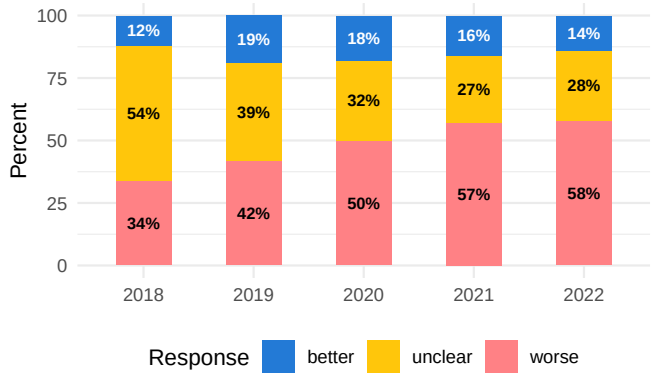
[481] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d)(2).

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

9.1.2: Unsafe Interactions

Do the policies clearly indicate whether or not a user can interact with untrusted users?

Figure 104: Unsafe Interactions



The Unsafe Interactions evaluation question indicates whether any users can have social interactions with other untrusted or unknown users, such as other users on the product who may be adults or children. A company should only provide unsafe interactions between adults to prevent inappropriate conversations between adults and children that could cause social, emotional, or physical harm.

Better Practice

Users cannot interact with untrusted users, including strangers and/or adults.

Worse Practice

Users can interact with untrusted users, including strangers and/or adults.

Statutes & Regulations:

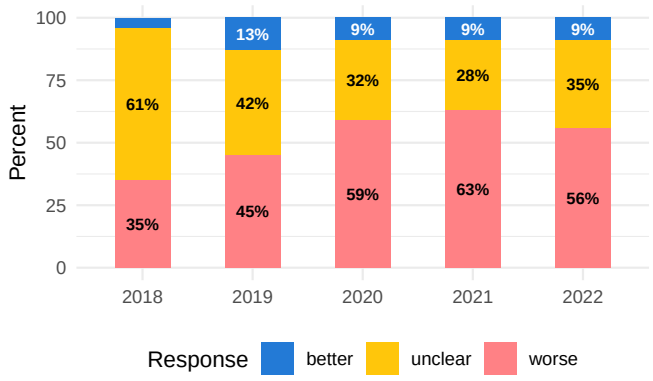
- COPPA: (An operator is required to disclose whether the service enables a child to make personal information publicly available.)[483]
- COPPA: (An operator is prohibited from making personal information from a child publicly available in identifiable form by any means, including a public posting through the Internet, or through a personal home page or screen posted on a Web site or online service, a pen pal service, an electronic mail service, a message board, or a chat room.)[484]

[483] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d)(2).
[484] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

9.1.3: Share Profile

Do the policies clearly indicate whether or not information must be shared or revealed by a user in order to participate in social interactions?

Figure 105: Share Profile



The Share Profile evaluation question indicates whether the user's profile information on the product must be shared with other users for social interactions. A company should limit the types of profile information that must be be shared with other users or publicly with privacy controls to prevent inadvertent disclosure of a user's identity that could cause social, emotional, or physical harm.

Better Practice

Profile information must be not shared for social interactions.

Worse Practice

Profile information must be shared for social interactions.

Statutes & Regulations:

- COPPA: (An operator is required to disclose whether the service enables a child to make personal information publicly available.) [485]

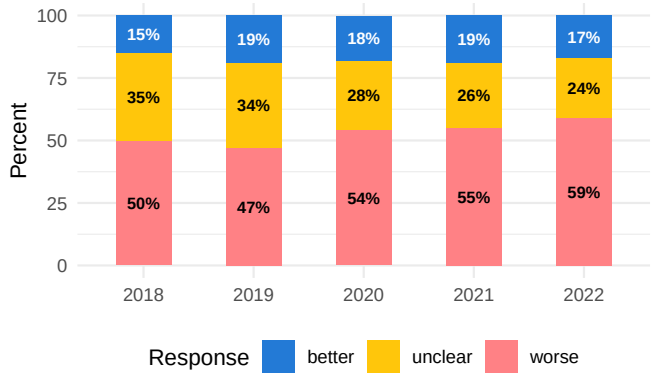
[485] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d)(2).

Data Visibility

9.2.1: Visible Data

Do the policies clearly indicate whether or not a user's personal information can be displayed publicly in any way?

Figure 106: Visible Data



The Visible Data evaluation question indicates whether a user's personal information can be made publicly available on the product to other unknown users, or publicly available online to anyone. A company should use privacy-by-design principles with default privacy controls that use the most privacy-protecting settings for a user's personal data that set visibility to ""private" on the product, which allows the user to change the visibility as needed. A company should also limit the types of profile information of children or students that can be shared with other users or publicly to prevent inadvertent disclosure of a user's identity that could cause social, emotional, or physical harm.

Better Practice

Personal information can be not displayed publicly.

Worse Practice

Personal information can be displayed publicly.

Statutes & Regulations:

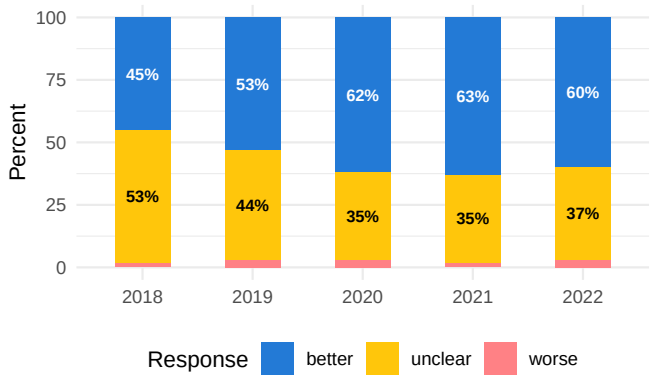
- COPPA: (An operator is required to disclose whether the service enables a child to make personal information publicly available.) [486]
- COPPA: (An operator is prohibited from making personal information from a child publicly available in identifiable form by any means, including a public posting through the Internet, or through a personal home page or screen posted on a Web site or online service, a pen pal service, an electronic mail service, a message board, or a chat room.) [487]

[486] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d)(2).
[487] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.2.

9.2.2: Control Visibility

Do the policies clearly indicate whether or not a user has control over how their personal information is displayed to others?

Figure 107: Control Visibility



The Control Visibility evaluation question indicates whether a user can control how their personal information is displayed to other users on the product or elsewhere online. A company should limit the types of profile information of children or students that can be shared with other users or publicly with privacy controls to prevent inadvertent disclosure of a user's identity that could cause social, emotional, or physical harm.

Better Practice

Users can control how their data are displayed to others.

Worse Practice

Users cannot control how their data are displayed to others.

Statutes & Regulations:

- CAADCA: (A business shall configure all default privacy settings provided to children by the online service, product, or feature to settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children.) [488]

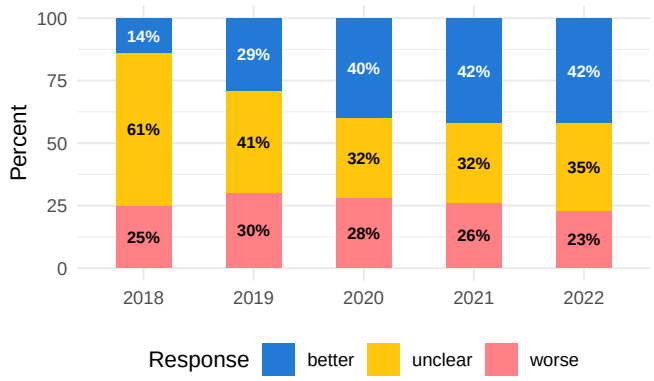
[488] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(a)(6).

Monitor and Review

9.3.1: Monitor Content

Do the policies clearly indicate whether or not the company reviews, screens, or monitors user-created content?

Figure 108: Monitor Content



The Monitor Content evaluation question indicates that the company has a process to review, screen, or monitor user-created content for inappropriate content. A company should have a content-moderation management system in place to prevent age-inappropriate content, or content that otherwise violates the respective policies from being shared between adults and children that could cause social, emotional, or physical harm.

Better Practice

User-created content is reviewed, screened, or monitored by the company.

Worse Practice

User-created content is not reviewed, screened, or monitored by the company.

Statutes & Regulations:

- DSA: (Providers of intermediary services shall make publicly available, in a machine-readable format and in an easily accessible manner, at least once a year, clear, easily comprehensible reports on any content moderation that they engaged in during the relevant period.) [489]
- CDA: (No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or any action taken to enable or make available to information content providers or others the technical means to restrict access to material.) [490]

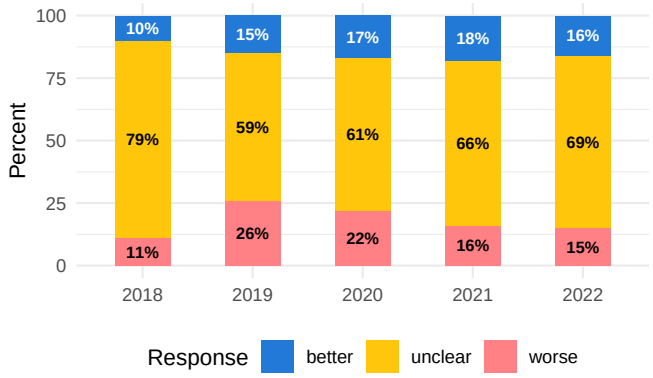
[489] Digital Services Act (Regulation (EU) 2022/2065), Transparency reporting obligations for providers of intermediary services, Art. 15(1).

[490] The Communications Decency Act of 1996 (CDA), 47 U.S.C. 230(c).

9.3.2: Filter Content

Do the policies clearly indicate whether or not the company takes reasonable measures to delete all personal information from a user's postings before they are made publicly visible?

Figure 109: Filter Content



The Filter Content evaluation question indicates that all personal information is deleted by the company from a child's or student's postings on the product before it is made public or available to other users. A company should have a content-filtering system in place to prevent personal information from children and students from being shared publicly or between adults and children that could cause social, emotional, or physical harm.

Better Practice

User-created content is filtered for personal information before being made publicly visible.

Worse Practice

User-created content is not filtered for personal information before being made publicly visible.

Statutes & Regulations:

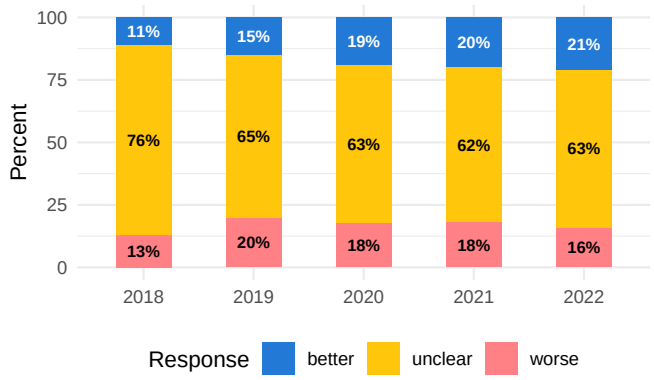
- COPPA: (An operator may prevent collection of personal information if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete the information from its records.)[491]

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

9.3.3: Moderating Interactions

Do the policies clearly indicate whether or not social interactions between users of the product may be moderated?

Figure 110: Moderating Interactions



The Moderating Interactions evaluation question indicates whether the company monitors and filters social interactions between users on the product. A company should have a social interaction filtering system in place to prevent personal information from children and students from being shared between adults and children as well as preventing abusive content that could cause social, emotional, or physical harm.

Better Practice

Social interactions between users are moderated.

Worse Practice

Social interactions between users are not moderated.

Statutes & Regulations:

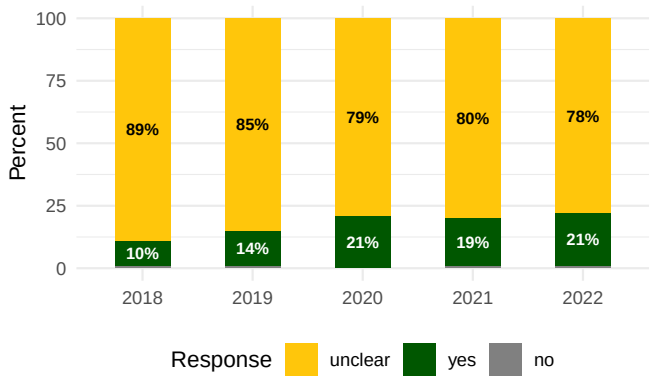
- COPPA: (An operator may prevent collection of personal information if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete the information from its records.) [492]
- COPPA: (An operator is prohibited from making personal information from a child publicly available in identifiable form by any means, including a public posting through the Internet, or through a personal home page or screen posted on a Web site or online service, a pen pal service, an electronic mail service, a message board, or a chat room.) [493]

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

9.3.4: Log Interactions

Do the policies clearly indicate whether or not social interactions, including private and direct messages, are logged by the company and are available for review or audit?

Figure 111: Log Interactions



The Log Interactions evaluation question indicates that social interactions between users on the product are logged by the company for safety purposes. A company that provides social interactions between users should log interactions only for a specified period of time to prevent inappropriate conversations between adults and children that could cause social, emotional, or physical harm. However, logging of children's or students' personal information, usage information, and behavioral information through the use of email, chat communications, and use of the product itself can increase the risk that the information may be used or disclosed in unintended ways.

Qualitative Status: Complex

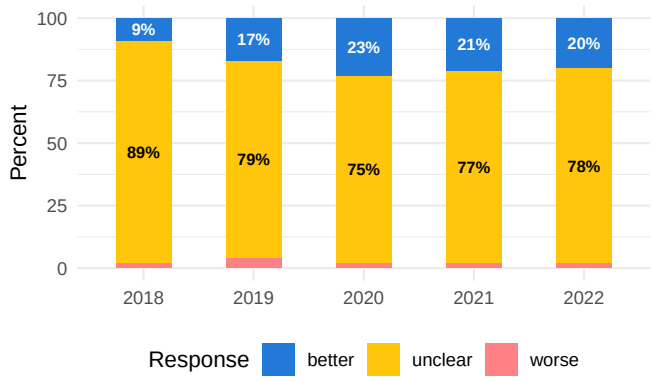
The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Report Content

9.4.1: Block Content

Do the policies clearly indicate whether or not an authorized user has the ability to filter or block inappropriate content?

Figure 112: Block Content



The Block Content evaluation question indicates that there is a process for the user, parent, or educator to temporarily or permanently block inappropriate content on the product from being displayed to children and students. A company should have a content-filtering system in place to prevent children and students from being exposed to obscene or inappropriate content that could cause social, emotional, or physical harm.

Better Practice

Users can filter or block inappropriate content.

Worse Practice

Users cannot filter or block inappropriate content.

Statutes & Regulations:

- CIPA: (A K-12 school under E-Rate discounts is required to adopt a policy of Internet safety for minors that includes monitoring the online activities of minors and the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access to visual depictions that are obscene, child pornography, or harmful to minors.) [494]
- CalPRMDW: (Prohibits an operator from marketing or advertising non age-appropriate types of products or services to a minor under 18 years of age and from knowingly using, disclosing, compiling, or allowing a third party to use, disclose, or compile, the personal information of a minor for the purpose of marketing or advertising non age-appropriate types of products or services. Also, a minor is permitted to request to "erase" or remove and obtain removal of content or information posted on the operator's site.) [495]
- CDA: (A provider of an interactive computer service shall notify the customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors.) [496]

[494] Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(h)(5)(B).

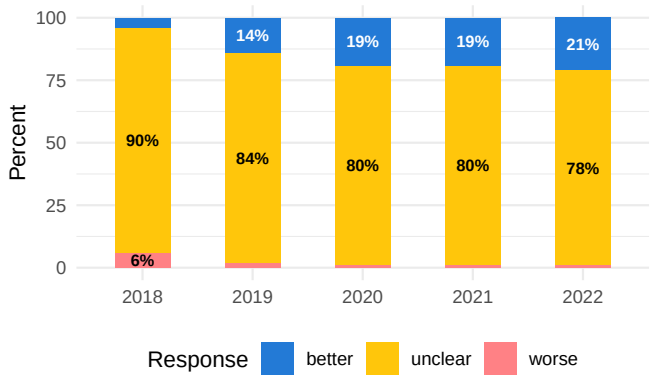
[495] California Privacy Rights for Minors in the Digital World, Cal. B.&P. Code §§ 22580-22582.

[496] The Communications Decency Act of 1996 (CDA), 47 U.S.C. 230(d).

9.4.2: Report Abuse

Do the policies clearly indicate whether or not inappropriate content, harassment, or cyberbullying can be reported?

Figure 113: Report Abuse



The Report Abuse evaluation question indicates that there is a process for the user, parent, or educator to temporarily or permanently block specific users on the product from displaying content or engaging in social interactions with other children and students. The ability to report abuse and cyberbullying is becoming increasingly important to teachers and parents in order to protect children who are spending more time online both in and out of school. A company should have a cyberbullying- or abuse-reporting mechanism in place to prevent children and students from being exposed to abuse that could cause social, emotional, or physical harm.

Better Practice

Users can report abuse or cyberbullying.

Worse Practice

Users cannot report abuse or cyberbullying.

Statutes & Regulations:

- CAADCA: (A business shall provide prominent, accessible, and responsive tools to help children, or their parents or guardians, exercise their privacy rights and report concerns.)[497]
- DSA: (Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content.)[498]

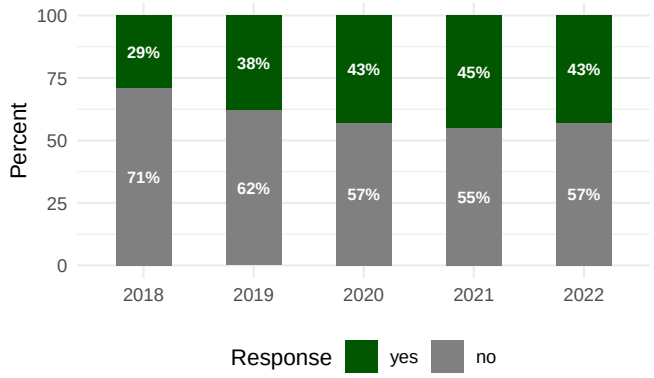
[497] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(a)(10).
[498] Digital Services Act (Regulation (EU) 2022/2065), Notice and action mechanisms, Art. 16(1).

Internet Safety

9.5.1: Safe Tools

Do the policies clearly indicate the company provides notice, resources, or processes that support safe and appropriate social interactions on the product?

Figure 114: Safe Tools



The Safe Tools evaluation question indicates that the company provides links to resources to help consumers, parents, and educators learn more about how to better protect their privacy on the product and the privacy of their children and students. Companies should prioritize the safety and privacy of their users with links to third-party resources to learn more how to become a better digital citizen and protect themselves online.

Transparent Practice

The company provides links to resources that support safe and appropriate social interactions.

Statutes & Regulations:

- CIPA: (A K-12 school under E-Rate discounts is required to adopt a policy of Internet safety for minors that includes monitoring the online activities of minors and the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access to visual depictions that are obscene, child pornography, or harmful to minors.) [499]
- CalPRMDW: (Prohibits an operator from marketing or advertising non age-appropriate types of products or services to a minor under 18 years of age and from knowingly using, disclosing, compiling, or allowing a third party to use, disclose, or compile, the personal information of a minor for the purpose of marketing or advertising non age-appropriate types of products or services. Also, a minor is permitted to request to "erase" or remove and obtain removal of content or information posted on the operator's site.) [500]
- CDA: (A provider of an interactive computer service shall notify the customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors.) [501]

[499] *See* Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(h)(5)(B).

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

[501] The Communications Decency Act of 1996 (CDA), 47 U.S.C. 230(d).

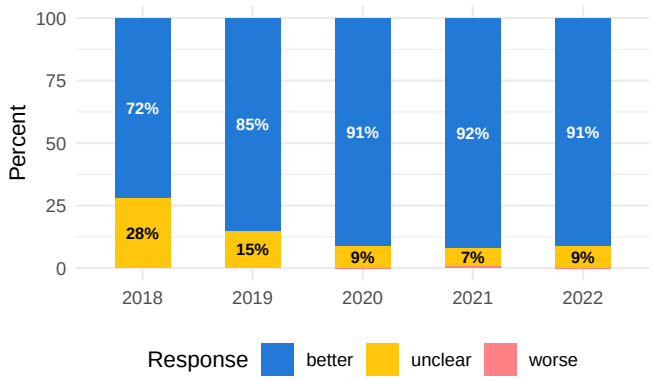
Advertising (How are Data used for Traditional, Contextual, or Behavioral Marketing?)

Company Communications

10.1.1: Service Messages

Do the policies clearly indicate whether or not a user may receive service- or administrative-related email or text message communications from the company or a third party?

Figure 115: Service Messages



The Service Messages evaluation question indicates that users may receive non-marketing communications from the company by email or mobile notifications to provide notice of important updates, service announcements, or changes to the policies or practices of the product.

Better Practice

A user can receive service- or administrative-related communications from the company.

Worse Practice

A user cannot receive service- or administrative-related communications from the company.

Statutes & Regulations:

- CCPA: ("Business purpose" means the use of personal information for the business's operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected.) [502]

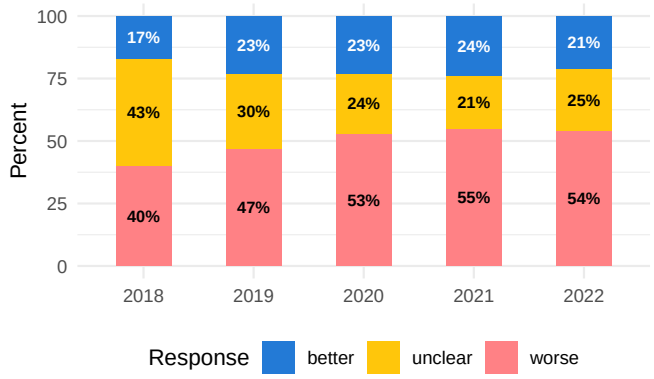
[502] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e).

Traditional Advertising

10.2.1: Contextual Ads

Do the policies clearly indicate whether or not traditional or contextual advertisements are displayed to a user based on a webpage's content, and not that user's data?

Figure 116: Contextual Ads



The Contextual or Traditional Advertisements evaluation question indicates whether advertisements are displayed to any users without using any collected personal information from the product. Traditional advertisements (otherwise referred to as contextual advertisements) display products and services to users based only on the relevant content or web page the user is currently viewing, but contextual ads do not collect any specific information about the user in order to display these ads.

Better Practice

Traditional or contextual advertisements are not displayed.

Worse Practice

Traditional or contextual advertisements are displayed.

Statutes & Regulations:

- COPPA: (An operator may display contextual advertisements to a child under the age of 13 without verifiable parental consent, under the "internal operations" exception.) [503]
- CCPA: ("Advertising and marketing" means a communication by a business or a person acting on the business's behalf in any medium intended to induce a consumer to obtain goods, services, or employment.) [504]
- CCPA: (Business purposes include auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.) [505]
- CCPA: (Business purposes include short-term, transient use, including but not limited to non-personalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.) [506]
- CCPA: ("Non-personalized advertising" means advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business, with the exception of the consumer's precise geolocation.) [507]
- DSA: (Providers of online platforms that present advertisements on their online interfaces shall ensure that, for each specific advertisement presented to each individual recipient, the recipients of the service are able to identify, in a clear, concise and unambiguous manner and in real time.) [508]
- CCPA: (A "business purpose" means providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer, provided that for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers which the service provider or contractor receives from or on behalf of the business with personal information which the service provider or contractor receives from or on behalf of another person or persons, or collects from its own interaction with consumers.) [509]

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

[504] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(a).

[505] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e)(1).

[506] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e)(4).

[507] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(t).

[508] Digital Services Act (Regulation (EU) 2022/2065), Advertising on online platforms, Art. 26.

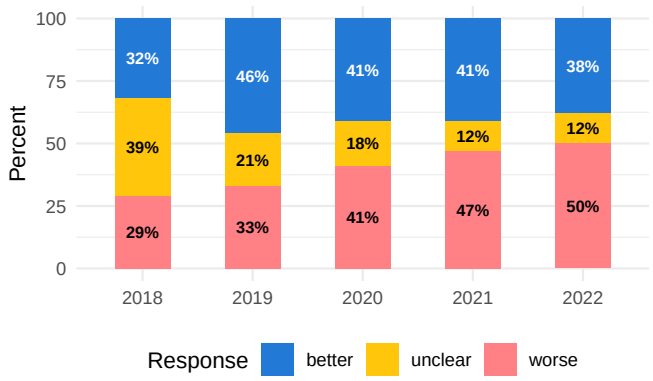
[509] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e)(6).

Behavioral Advertising

10.3.1: Personalised Ads

Do the policies clearly indicate whether or not advertising based on a user's personal information are displayed on the first-party product?

Figure 117: Personalised Ads



The Personalised Ads evaluation question indicates whether advertisements are displayed to any users based on collected personal information or behavioral information on how users use the product also known as behavioral or targeted advertisements. Personalised advertisements take targeted advertisements one step further, collecting specific information about users typically through the use of cookies, beacons, tracking pixels, persistent identifiers, or other tracking technologies that provide more specific information over time about the user. This information is then shared with advertisers, who display even more targeted products and services than targeted advertisements to the user based on the behavioral information they received from the user's activities on the product.

Better Practice

Personalised advertising is not displayed.

Worse Practice

Personalised advertising is displayed.

Statutes & Regulations:

- COPPA: (An operator is prohibited from including behavioral advertisements or amassing a profile of a child under the age of 13 child without parental consent.) [510]
- SOPIPA: (An operator is prohibited from using student data for targeted advertising.) [511]
- CCPA: ("Share," "shared," or "sharing" 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.) [512]
- DSA: (Providers of online platforms that present advertisements on their online interfaces shall ensure that, for each specific advertisement presented to each individual recipient, the recipients of the service are able to identify, in a clear, concise and unambiguous manner and in real time.) [513]
- AB 1584: (A local educational agency that enters into a contract with a third party must ensure the contract contains a prohibition against the third party using personally identifiable information in pupil records to engage in targeted advertising.) [514]

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

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

[512] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ah).

[513] Digital Services Act (Regulation (EU) 2022/2065), Advertising on online platforms, Art. 26.

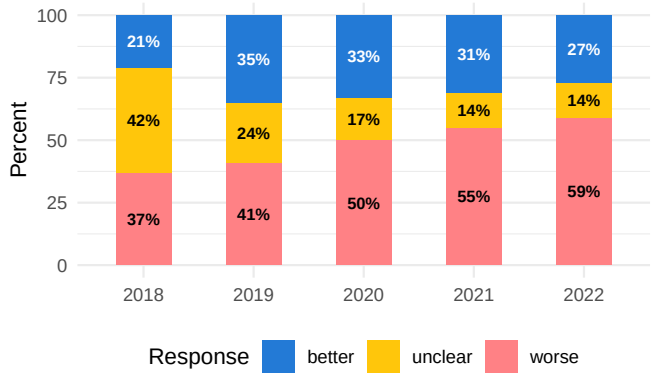
[514] California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(9).

Ad Tracking

10.4.1: 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 118: Third-Party Tracking



The Third-Party Tracking evaluation question indicates whether the company allows third-party companies to use cookies or other tracking technologies on its product, which enables those third parties 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 while 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 processes without their knowledge, which may cause unintended harm.

Better Practice

Data are not collected by third-parties for their own purposes.

Worse Practice

Data are collected by third-parties for their own purposes.

Statutes & Regulations:

- SOPIPA: (An operator is prohibited from tracking a student across websites with targeted advertising.) [515]
- COPPA: (An operator is prohibited from sharing a persistent identifier collected from children that can be used to recognize and track a user over time and across different websites or services without verifiable parental consent.) [516]
- CalOPPA: (An operator may provide a hyperlink in their privacy policy to a location containing a description, including the effects, of any program or protocol that offers the consumer a choice not to be tracked.) [517]
- CCPA: ("Cross-context behavioral advertising" means 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.) [518]
- CCPA: ("Share," "shared," or "sharing" 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.) [519]
- CCPA: ("Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer or family. For purposes of this subdivision, "family" means a custodial parent or guardian and any children under 18 years of age over which the parent or guardian has custody.) [520]

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

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

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

[518] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(k).

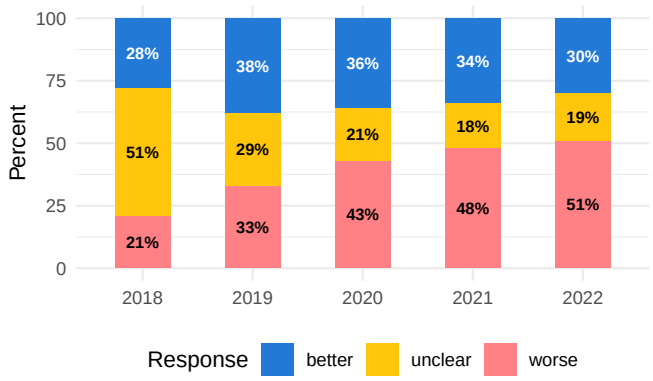
[519] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ah).

[520] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(aj).

10.4.2: Track Users

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

Figure 119: Track Users



The Track Users evaluation question indicates that the product uses cookies or other tracking technologies on its service for the specific purpose of allowing third-party companies to display advertisements to the service'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.

Better Practice

User's information is not used to track and target advertisements on other third-party websites or services.

Worse Practice

User's information is used to track and target advertisements on other third-party websites or services.

Statutes & Regulations:

- COPPA: (An operator is prohibited from sharing a persistent identifier collected from children that can be used to recognize and track a user over time and across different websites or services without verifiable parental consent.)[521]
- SOPIPA: (An operator is prohibited from tracking a student across websites with targeted advertising.)[522]
- CalOPPA: (An operator is required to disclose whether other third parties may collect personally identifiable information about a consumer's online activities over time and across different Websites.)[523]
- FERPA: ("Personal Information" under FERPA includes direct identifiers such as a student or family member's name, or indirect identifiers such as a date of birth, or mother's maiden name, or other information that is linkable to a specific student that would allow a reasonable person in the school community to identify the student with reasonable certainty.)[524]
- CalPRMDW: (Prohibits an operator from marketing or advertising non age-appropriate types of products or services to a minor under 18 years of age and from knowingly using, disclosing, compiling, or allowing a third party to use, disclose, or compile, the personal information of a minor for the purpose of marketing or advertising non age-appropriate types of products or services. Also, a minor is permitted to request to "erase" or remove and obtain removal of content or information posted on the operator's site.)[525]
- CCPA: (Business purposes include short-term, transient use, including but not limited to non-personalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.)[526]
- CCPA: ("Cross-context behavioral advertising" means 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.)[527]
- CCPA: ("Share," "shared," or "sharing" 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-

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

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

[523] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(6).

[524] *See* Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.

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

[526] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e)(4).

[527] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(k).

context behavioral advertising for the benefit of a business in which no money is exchanged.)[528]

- CCPA: ("Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer or family. For purposes of this subdivision, "family" means a custodial parent or guardian and any children under 18 years of age over which the parent or guardian has custody.)[529]
- CAADCA: (A business shall not collect, sell, "share", or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, unless the business can demonstrate a compelling reason that the collecting, selling, sharing, or retaining of the personal information is in the best interests of children.)[530]

[528] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(ah).

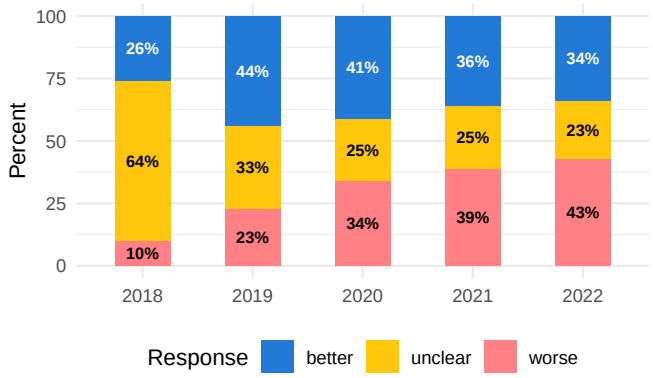
[529] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(aj).

[530] *See* California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(b)(3).

10.4.3: 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 personalised advertising?

Figure 120: Ad Profile



The Ad Profile evaluation question indicates whether a product allows third-party companies to create a behavioral profile about a user based on the user's personal information for advertising or marketing purposes across the internet. A company should not 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 audience segment or profile. Automated decision-making, including the creation of profiles for tracking or advertising purposes, can lead to an increased risk of harmful outcomes that may disproportionately and significantly affect children or students.

Better Practice

Data profiles are not created and used for personalised advertisements.

Worse Practice

Data profiles are created and used for personalised advertisements.

Statutes & Regulations:

- COPPA: (An operator is prohibited from including behavioral advertisements or amassing a profile of a child under the age of 13 child without parental consent.) [531]
- SOPIPA: (An operator is prohibited from amassing a profile of a student.) [532]
- SOPIPA: (An operator may share student data with third parties for legitimate research purposes if not used for advertising or to amass a profile on a student for purposes other than K–12 school purposes.) [533]
- CalPRMDW: (Prohibits an operator from marketing or advertising non age-appropriate types of products or services to a minor under 18 years of age and from knowingly using, disclosing, compiling, or allowing a third party to use, disclose, or compile, the personal information of a minor for the purpose of marketing or advertising non age-appropriate types of products or services. Also, a minor is permitted to request to "erase" or remove and obtain removal of content or information posted on the operator's site.) [534]
- GDPR: (The controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: ... (f) the existence of automated decision-making, including profiling ... and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.) [535]
- GDPR: (The controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: ... (g) the existence of automated decision-making, including profiling ... and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.) [536]
- GDPR: (The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: ... (h) the existence of automated decision-making, including profiling ... and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.) [537]
- GDPR: (The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.) [538]

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

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

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

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

[535] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(2)(f).

[536] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(g).

[537] General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(1)(h).

[538] General Data Protection Regulation (GDPR) 2016/679, Automated individual decision-making, including profiling, Art. 22(1).

- GDPR: (Automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her shall be permitted if ... based on the data subject's explicit consent.) [539]
- GDPR: (the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.) [540]
- GDPR: ("profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.) [541]
- CCPA: (Business purposes include short-term, transient use, including but not limited to non-personalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.) [542]
- CCPA: ("Personal information" includes inferences drawn from any information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.) [543]
- CCPA: ("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.) [544]
- CCPA: ("Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer or family. For purposes of this subdivision, "family" means a custodial parent or guardian and any children under 18 years of age over which the parent or guardian has custody.) [545]
- CAADCA: (The term "profiling" means any form of automated processing of personal information that uses personal information to evaluate certain aspects relating to a natural person, including analyzing or predicting aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.) [546]
- CAADCA: (A business shall not profile a child by default unless the business can demonstrate it has appropriate safeguards in place to protect children, and profiling is necessary to provide the online service, product, or feature requested, or the business can demonstrate a compelling reason that profiling is in the best interests of children.) [547]
- DSA: (Providers of online platforms shall not present advertisements to recipients of the service based on profiling using special categories of personal data referred to in the GDPR.) [548]
- DSA: (Providers of online platforms shall not present advertisements on their interface based on profiling using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor.) [549]

[539] General Data Protection Regulation (GDPR) 2016/679, Automated individual decision-making, including profiling, Art. 22(2)(c).

[540] General Data Protection Regulation (GDPR) 2016/679, Automated individual decision-making, including profiling, Art. 22(3).

[541] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(4).

[542] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(e)(4).

[543] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(v)(1)(K).

[544] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(z).

[545] *See* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(aj).

[546] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.30(b)(6).

[547] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(b)(2)(A)-(B).

[548] Digital Services Act (Regulation (EU) 2022/2065), Advertising on online platforms, Art. 26(3).

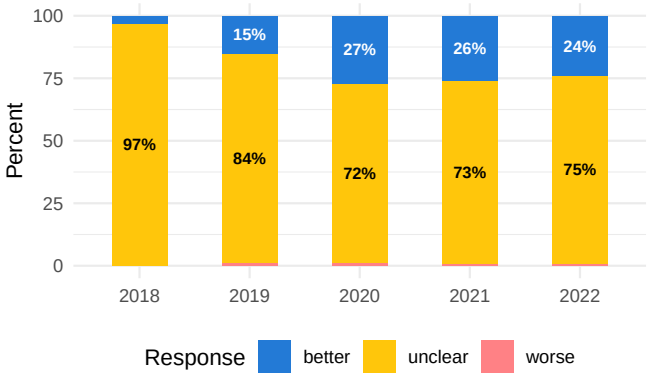
[549] Digital Services Act (Regulation (EU) 2022/2065), Online protection of minors, Art. 28(2).

Filtered Advertising

10.5.1: Filter Ads

Do the policies clearly indicate whether or not the company or third party filters advertisements for kids (e.g., no alcohol, gambling, violence, or sexual content)?

Figure 121: Filter Ads



The Filter Ads evaluation question indicates that age-inappropriate advertisements (e.g., alcohol, smoking, gambling, violence, or sexual content) are excluded from the product if used by children or students. A child's personal information provided to a product should not be used to exploit that user's specific knowledge, traits, and viewing behaviors to influence their desire to purchase goods and services that are inappropriate for minors.

Better Practice

Ads displayed to children are filtered for inappropriate content.

Worse Practice

Ads displayed to children are not filtered for inappropriate content.

Statutes & Regulations:

- CalPRMDW: (Prohibits an operator from marketing or advertising non age-appropriate types of products or services to a minor under 18 years of age and from knowingly using, disclosing, compiling, or allowing a third party to use, disclose, or compile, the personal information of a minor for the purpose of marketing or advertising non age-appropriate types of products or services. Also, a minor is permitted to request to "erase" or remove and obtain removal of content or information posted on the operator's site.) [550]
- CIPA: (A K-12 school under E-Rate discounts is required to adopt a policy of Internet safety for minors that includes monitoring the online activities of minors and the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access to visual depictions that are obscene, child pornography, or harmful to minors.) [551]
- CAADCA: (The term "likely to be accessed by children" means it is reasonable to expect that the online service, product, or feature would be accessed by children, if the online service, product, or feature displays advertisements marketed to children.) [552]

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

[551] Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(h)(5)(B).

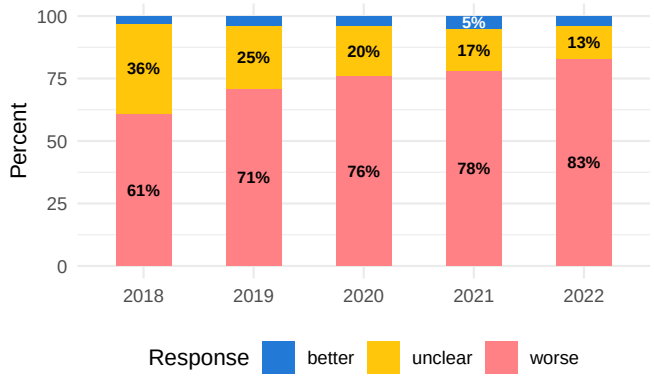
[552] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.30(b)(4)(C).

Marketing Communications

10.6.1: Company's Marketing

Do the policies clearly indicate whether or not the company may send marketing emails, text messages, or other related communications that may be of interest to a user?

Figure 122: Company's Marketing



The Company's Marketing evaluation question indicates the company sends first-party marketing emails, text messages, or other related communications to its users for advertising purposes. A company should not send first-party marketing messages to children or students. Any marketing communications should only be sent to adult users of the product if explicit opt-in consent was obtained for that purpose.

Better Practice

The company cannot send marketing messages.

Worse Practice

The company can send marketing messages.

Statutes & Regulations:

- COPPA: (An operator may display contextual advertisements to a child under the age of 13 without verifiable parental consent, under the "internal operations" exception.) [553]
- CalPRMDW: (Prohibits an operator from marketing or advertising non age-appropriate types of products or services to a minor under 18 years of age and from knowingly using, disclosing, compiling, or allowing a third party to use, disclose, or compile, the personal information of a minor for the purpose of marketing or advertising non age-appropriate types of products or services. Also, a minor is permitted to request to "erase" or remove and obtain removal of content or information posted on the operator's site.) [554]
- CCPA: ("Non-personalized advertising" means advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business, with the exception of the consumer's precise geolocation.) [555]
- Telecom Act: (A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall not use customer information for its own marketing efforts.) [556]

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

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

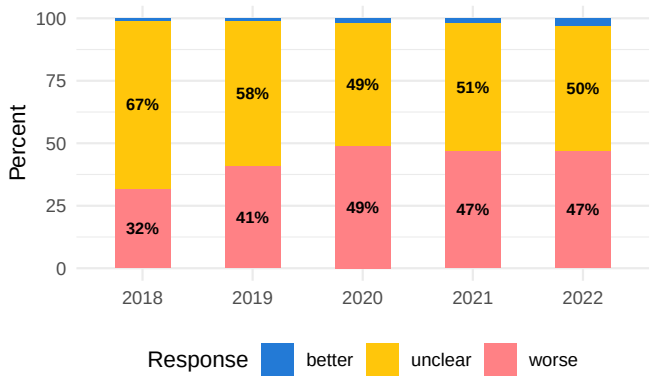
[555] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(t).

[556] Telecommunications Act, Privacy of customer information, 47 U.S. Code § 222(b).

10.6.2: Third-Party Promotions

Do the policies clearly indicate whether or not the company may ask a user to participate in any third-party sweepstakes, contests, surveys, or other similar promotions?

Figure 123: Third-Party Promotions



The Third-Party Promotions evaluation question indicates that the company may send its own first-party or third-party promotional sweepstakes, contests, or surveys to users of the product. A company should not encourage the submission of personal information with the use of promotions, prizes, or games.

Better Practice

The company does not provide promotional sweepstakes, contests, or surveys.

Worse Practice

The company does provide promotional sweepstakes, contests, or surveys.

Statutes & Regulations:

- COPPA: (A vendor is prohibited from conditioning a child's participation in a game or prize on the child disclosing more info than necessary to participate in the activity.) [557]
- COPPA: (A vendor may not request, prompt, entice, or encourage the submission of PII with the use of prizes or games.) [558]
- PPRA: (All instructional materials including teacher's manuals, films, tapes, or other supplementary instructional material which is used in connection with any research must be made available for inspection by the parents or guardians of the children.) [559]
- CAADCA: (A business shall not collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, unless the business can demonstrate a compelling reason that the collecting, selling, sharing, or retaining of the personal information is in the best interests of children.) [560]

[557] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.7.

[558] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(d).

[559] Protection of Pupil Rights Act (PPRA), 34 C.F.R. §98.3.

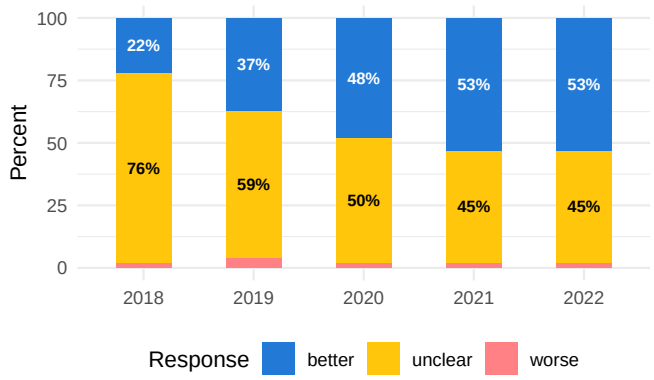
[560] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(b)(3).

Unsubscribe

10.7.1: Unsubscribe Ads

Do the policies clearly indicate whether or not a user can opt out of any advertising?

Figure 124: Unsubscribe Ads



The Unsubscribe Ads evaluation question indicates that the company provides users with the ability to opt-out from first-party or third-party advertising on the product. A company should provide privacy controls for users to easily opt-out of personalised advertising to users based on their personal information.

Better Practice

Users can opt out of contextual, or personalised advertising.

Worse Practice

Users cannot opt out of contextual, or personalised advertising.

Statutes & Regulations:

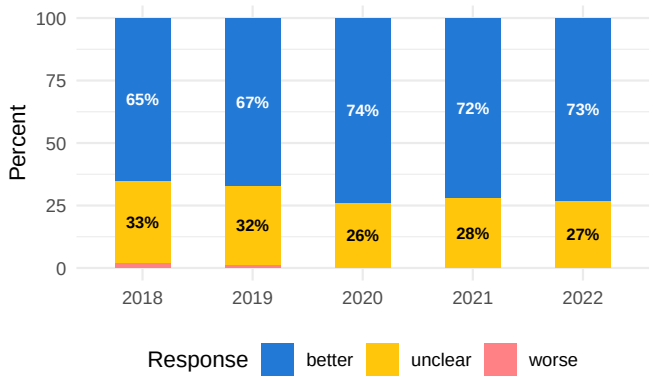
- COPPA: (An operator can not condition a child's participation in the service by sharing any collected information with third parties. A parent is required to have the ability to consent to the collection and use of their child's personal information without also consenting to the disclosure of the information to third parties.)[561]

[561] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(a)(2).

10.7.2: Unsubscribe Marketing

Do the policies clearly indicate whether or not a user can opt out or unsubscribe from a company or third party marketing communication?

Figure 125: Unsubscribe Marketing



The Unsubscribe Marketing evaluation question indicates that the company provides users with the ability to opt-out from first-party or third-party marketing communications. A company should provide privacy controls for users to easily opt-in or opt-out of different marketing uses of their personal information.

Better Practice

Users can opt out or unsubscribe from marketing communications.

Worse Practice

Users cannot opt out or unsubscribe from marketing communications.

Statutes & Regulations:

- CAN-SPAM: (The sender of a commercial electronic communication may not require that any recipient pay any fee, provide any information other than the recipient's electronic mail address and opt-out preferences, or take any other steps except sending a reply electronic mail message or visiting a single Internet Web page, in order to submit a request not to receive future commercial electronic mail messages from the sender.) [562]
- GDPR: (Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.) [563]
- GDPR: (Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.) [564]
- ShineTheLight: (California's "Shine the Light" refers to information sharing disclosure requirements for companies that do business with California residents to allow customers to opt-out of information sharing, or make a detailed disclosure of how personal information was shared for direct marketing purposes.) [565]

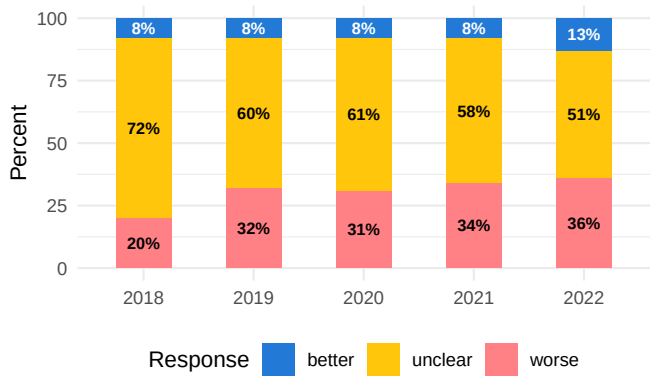
[562] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), 16 C.F.R. Part 316.5.
[563] General Data Protection Regulation (GDPR) 2016/679, Automated individual decision-making, including profiling, Art. 21(2).
[564] General Data Protection Regulation (GDPR) 2016/679, Automated individual decision-making, including profiling, Art. 21(3).
[565] Information Sharing Disclosure, Cal. Civ. Code §§ 1798.83-1798.84.

Do Not Track

10.8.1: DoNotTrack Response

Do the policies clearly indicate whether or not the company responds to a “Do Not Track” signal or other opt-out mechanisms from a user?

Figure 126: DoNotTrack Response



The DoNotTrack Response evaluation question indicates whether the product responds to a user's browser-based “Do Not Track” signal that provides notice to the company that the user requests to exercise their right to opt out of third-party tracking on the product.

Better Practice

Company does respond to “Do Not Track” or other opt-out mechanisms.

Worse Practice

Company does not respond to “Do Not Track” or other opt-out mechanisms.

Statutes & Regulations:

- CalOPPA: (An operator is required to disclose how they respond to Web browser “Do Not Track” signals or other mechanisms that provide consumers the ability to opt-out of the collection of personally identifiable information about their online activities over time and across third-party Web sites.) [566]
- CCPA: (A business that sells or shares consumers' personal information or uses or discloses consumers' sensitive personal information shall in a form that is reasonably accessible to consumers provide a clear and conspicuous link on the business's internet homepage(s), titled “Do Not Sell or Share My Personal Information,” to an internet webpage that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or sharing of the consumer's personal information. A business shall not be required to comply if the business allows consumers to opt-out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism to the business indicating the consumer's intent to opt-out of the business's sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information, or both.) [567]
- CCPA: (Issuing regulations shall define the requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt-out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information. The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses.) [568]

[566] California Online Privacy Protection Act (CalOPPA), Cal. B.&P. Code §22575(b)(5).

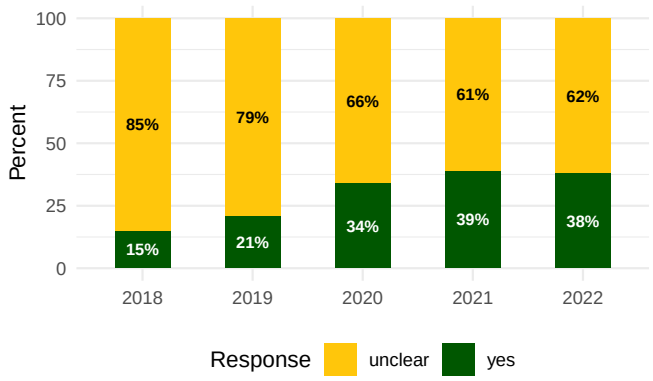
[567] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.135(a)-(b).

[568] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.185(19)(A).

10.8.2: DoNotTrack Description

Do the policies clearly indicate whether the company provides a link to a description and the effects of any program or protocol the company follows that offers consumers a choice not to be tracked?

Figure 127: DoNotTrack Description



The DoNotTrack Description evaluation question indicates that a hyperlink is available in the product's privacy policy to a location containing an alternative opt-out method not to be tracked by the product.

Transparent Practice

The company does provide a method for users to opt-out from third-party tracking.

Statutes & Regulations:

- CalOPPA: (An operator may provide a hyperlink in their privacy policy to a location containing a description, including the effects, of any program or protocol that offers the consumer a choice not to be tracked.) [569]

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

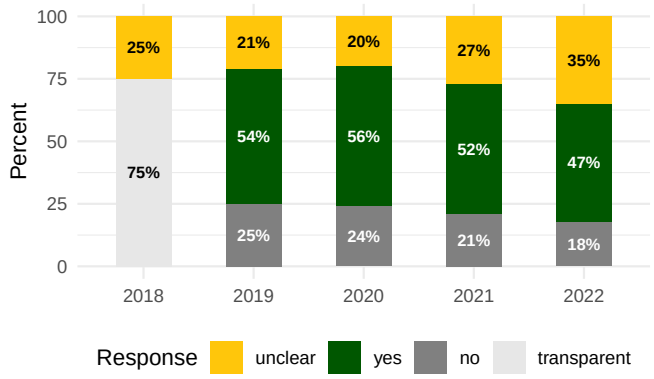
Compliance (How do Statutes and Regulations apply?)

Children Under 13

11.1.1: Actual Knowledge

Do the policies clearly indicate whether or not the company has actual knowledge that personal information from children under 13 years of age is collected by the product?

Figure 128: Actual Knowledge



The Actual Knowledge evaluation question indicates that the company has actual knowledge that users of the product are under the age of 13 because the product utilizes an age-gate or a user's birthday is collected upon account registration in the product. If a company has actual knowledge that a user is under the age of 13, then the product should apply additional privacy protections to children using the product.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

- COPPA: (A general audience site is where the operator has no actual knowledge that a child under the age of 13 has registered an account or is using the service, and no age gate or parental consent is required before collection of information.) [570]
- COPPA: (A mixed audience site is where the site is directed to children, but does not target children as its "primary audience," but rather teens 13-to-18 years of age or adults. An operator of a mixed audience site is required to obtain age information from a user before collecting any information and if a user identifies themselves as a child under the age of 13, the operator must obtain parental consent before any information is collected.) [571]
- COPPA: (A site directed to children is where the operator has actual knowledge the site is collecting information from children under the age of 13 and parental consent is required before any collection or use of information.) [572]
- COPPA: (A vendor who may obtain actual knowledge that it is collecting information from a child must not encourage a child from disclosing more information than reasonably necessary through an age verification mechanism. An age gate should be: age-neutral; not encourage falsification; list day, month, and year; have no prior warning that under 13 children will be blocked; and prevent multiple attempts.) [573]
- CCPA: (A business shall not sell or share the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.) [574]
- CAADCA: (A business shall not use any personal information collected to estimate age or age range for any other purpose or retain that personal information longer than necessary to estimate age. Age assurance shall be proportionate to the risks and data practice of an online service, product, or feature.) [575]
- DSA: (Compliance with the DSA shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor.) [576]

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

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

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

[573] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(d).

[574] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.120(c)-(d).

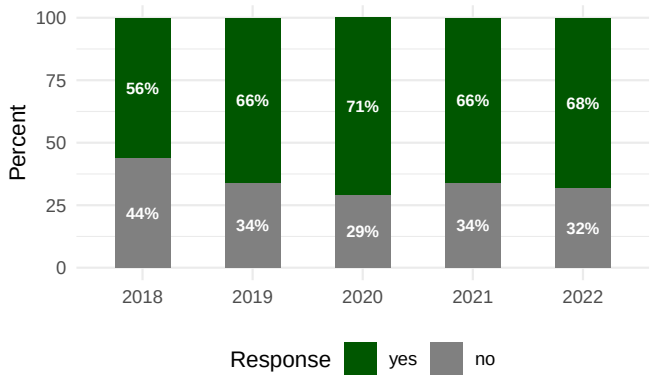
[575] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.31(b)(8).

[576] Digital Services Act (Regulation (EU) 2022/2065), Online protection of minors, Art. 28(3).

11.1.2: Children's Privacy

Does the company clearly provide a section or heading for children in their policies, or provide a separate kid's privacy policy or COPPA notice for kids?

Figure 129: Children's Privacy



The Children's Privacy evaluation question indicates that the policies have a separate section, heading, or a separate children's privacy policy. A company should provide a separate section or separate children's privacy statement that specifies the different data collection, use, and disclosure practices that apply to children using the product when children are an intended audience.

Transparent Practice

The company does provide a section, heading, or separate policy for children in their policies.

Statutes & Regulations:

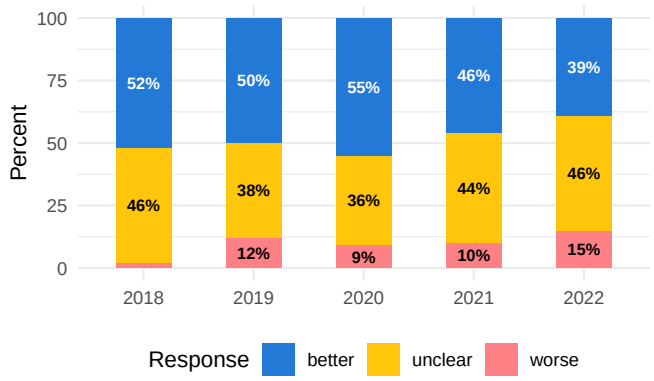
- COPPA: (A vendor is required to provide a clear privacy policy about: (1) what information is collected, (2) how information is used, and (3) its disclosure practices of that information.)[577]
- COPPA: (A notice or privacy policy on an operator's website needs a section relating to the collection of information for children under 13 years of age, and notice is required at each area of the site where information is collected from children.)[578]
- CAADCA: (If a conflict arises between a company's commercial interests and the best interests of children, companies should prioritize the privacy, safety, and well-being of children over commercial interests.)[579]
- DSA: (Providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service.)[580]

[577] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(a); See also 16 C.F.R. Part 312.4(d)(2).
[578] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(d).
[579] California Age-Appropriate Design Code Act (CAADCA), Cal. Civ. Code § 1798.99.29(b).
[580] Digital Services Act (Regulation (EU) 2022/2065), Online protection of minors, Art. 28(1).

11.1.3: Child-Prohibited Account

Do the policies clearly indicate whether or not the company restricts or prohibits creating an account for a child under 13 years of age?

Figure 130: Child-Prohibited Account



The Child-Prohibited Account evaluation question indicates that the product provides restrictions or prohibits the account creation of children under 13 years of age through use of an age-gate or collection of a user's birthday upon account registration. A company should restrict account creation by children to ensure parents register accounts for themselves and their children. Account restriction may allow parents to create a child profile which may provide better privacy-protecting data collection and use practices to users who use the managed account or profile.

Better Practice

Account creation is restricted or prohibited for users under 13 years of age.

Worse Practice

Account creation is not restricted or prohibited for users under 13 years of age.

Statutes & Regulations:

- COPPA: (No account registration for a child under 13 years of age is permitted without obtaining parental consent beforehand.)[581]

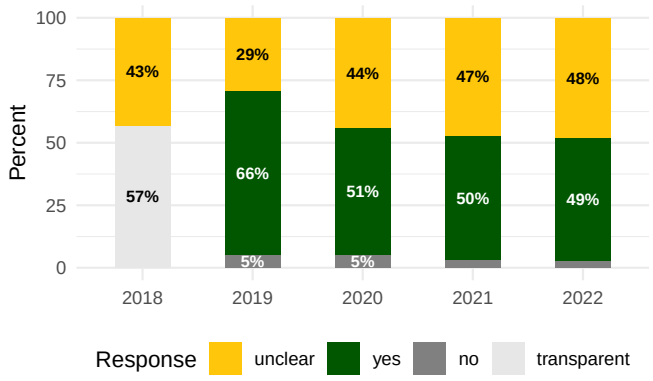
[581] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(b); See also 16 C.F.R. Part 312.5(a).

Students in K–12

11.2.1: School Purpose

Do the policies clearly indicate whether or not the product is primarily used, designed, and marketed for preschool or K-12 school purposes?

Figure 131: School Purpose



The School Purpose evaluation question indicates whether the product is primarily designed, marketed, and used for preschool or K-12 school purposes. A company should disclose whether the product is intended to be used in K-12 schools or districts because additional student data privacy laws apply to personal information collected from students.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

- SOPIPA: (SOPIPA applies to operators of online services that are primarily used for K-12 school purposes and were designed and marketed for K-12 school purposes.) [582]
- SOPIPA: (SOPIPA does not apply to general audience websites and services that are not primarily used by K-12 students.) [583]
- ELPIPA: (ELPIPA applies to operators of online services that are primarily used for preschool or prekindergarten purposes and were designed and marketed for preschool or prekindergarten purposes.) [584]
- FERPA: (FERPA applies to all educational institutions that accept public funds under a program of the U.S. Department of Education.) [585]
- SOPIPA: ("K–12 school purposes" means purposes that customarily take place at the direction of the K–12 school, teacher, or school district or aid in the administration of school activities, including instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school.) [586]

[582] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(a).

[583] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(m).

[584] Early Learning Personal Information Protection Act (ELPIPA), Cal. B.&P. Code § 22586(a)(1).

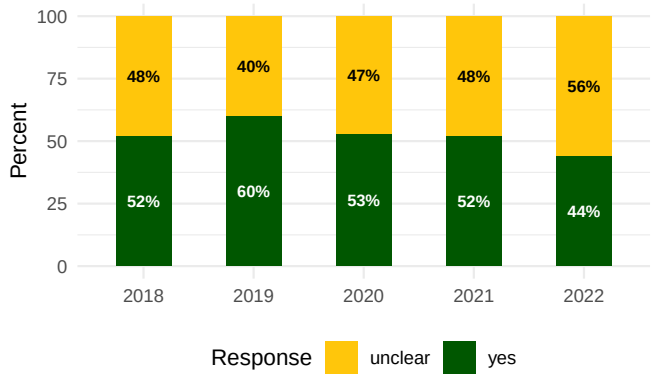
[585] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.1.

[586] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(j)

11.2.2: Education Records

Do the policies clearly indicate the process by which education records are entered into the product? For example, are student data entered by district staff, school employees, parents, teachers, students, or some other person?

Figure 132: Education Records



The Education Records evaluation question indicates whether the product explains how educational records are entered into the product which allows the collection of data from students to become protected educational records as part of an educational school or district program.

Transparent Practice

Processes to enter education records into the product are described.

Statutes & Regulations:

- FERPA: ("Education Records" are information that is directly related to a student and maintained by the educational institution, or by a third party acting as a School Official on behalf of the educational institution.) [587]
- CCPA: ("Personal Information" includes education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).) [588]

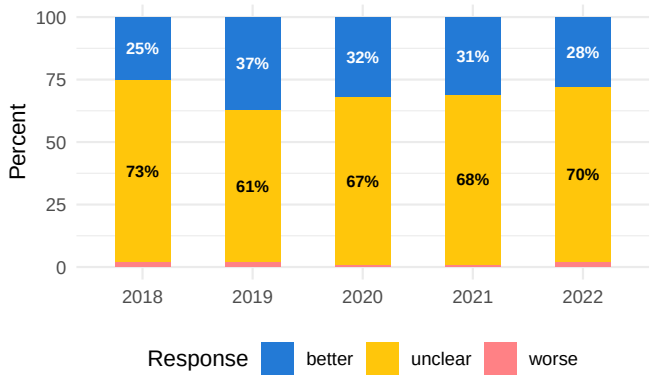
[587] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.3.

[588] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(v)(1)(J).

11.2.3: School Contract

Do the policies clearly indicate whether or not the company provides a contract to a Local Educational Agency (LEA)?

Figure 133: School Contract



The School Contract evaluation question indicates that the company provides a contract or student data privacy agreement to a local education agency to protect student data on the product. A company should put in place additional student data privacy protections that are not disclosed in the privacy policy in contractual agreements with schools and districts to ensure student's data is collected and used only for educational purposes.

Better Practice

Additional rights or protections may be provided with an additional school contract.

Worse Practice

Additional rights or protections are not provided with an additional school contract.

Statutes & Regulations:

- FERPA: (An educational institution must annually notify parents of their rights to inspect and review a student's education records, make corrections, delete, or consent to the disclosure of information.) [589]
- FERPA: (Any rights to access, modify, or delete student records may transfer to an "eligible" student who is over 18 years of age.) [590]
- GDPR: (The controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: ... (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.) [591]
- AB 1584: (Authorizes a Local Educational Agency (LEA) to enter into a third party contract for the collection and use of pupil records that must include a statement that the pupil records continue to be the property of and under the control of the local educational agency, a description of the actions the third party will take to ensure the security and confidentiality of pupil records, and a description of how the local educational agency and the third party will jointly ensure compliance with FERPA.) [592]

[589] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.7(a).

[590] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.5(a)(1).

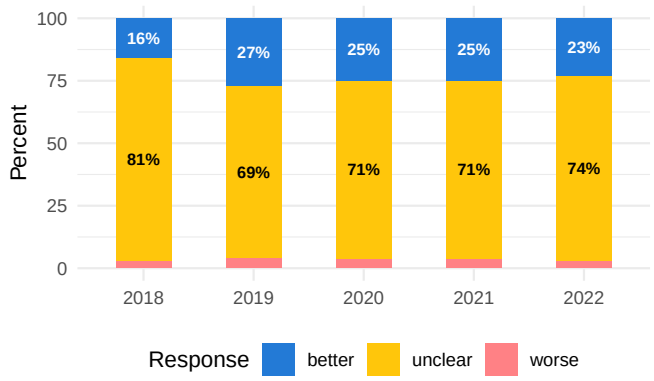
[591] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(2)(e).

[592] California Privacy of Pupil Records, Cal. Ed. Code §§ 49073.1.

11.2.4: School Official

Do the policies clearly indicate whether or not the company is under the direct control of the educational institution and designates themselves a 'School Official' under FERPA?

Figure 134: School Official



The School Official evaluation question indicates the company does operate under the direct control of any educational institution in which it has entered into a contractual agreement with and is designated a School Official under FERPA.

Better Practice

Company is designated as a school official.

Worse Practice

Company is not designated as a school official.

Statutes & Regulations:

- FERPA: (An exception for disclosing personally identifiable information without obtaining parental consent exists for sharing data with a third party who is considered a “school official” with a legitimate educational interest, and under direct control of the school for the use and maintenance of education records.) [593]
- FERPA: (An exception for disclosing personally identifiable information without obtaining parental consent exists for sharing with other school officials, including teachers within the same educational institution.) [594]
- FERPA: (An educational institution must use reasonable methods to ensure that school officials only use information for which they have a legitimate educational interest.) [595]
- AB 1584: (A local educational agency that enters into a contract with a third party must ensure the contract contains a description of how the local educational agency and the third party will jointly ensure compliance with the federal Family Educational Rights and Privacy Act (FERPA).) [596]

[593] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(i)(B).

[594] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(i)(A).

[595] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(a)(1)(ii).

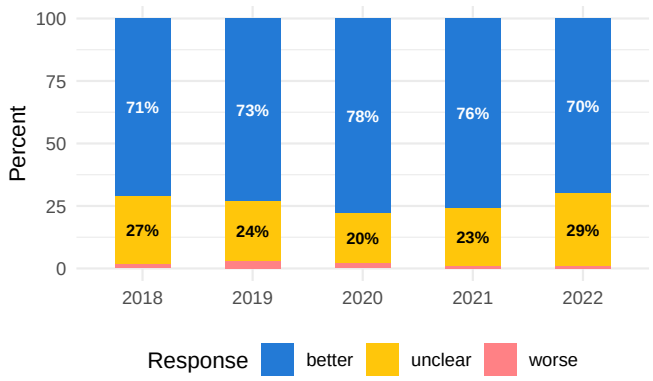
[596] California Privacy of Pupil Records, Cal. Ed. Code § 49073.1(b)(8).

Parental Consent

11.3.1: Parental Consent

Do the policies clearly indicate whether or not the company or a third party obtains verifiable parental consent before they collect or disclose personal information?

Figure 135: Parental Consent



The Parental Consent evaluation question indicates that the company obtains verifiable parental consent before they collect, use, or disclose any child or student's personal information. A company should disclose how information is collected from children and how that information is used in order to obtain informed parental consent, because there is an increased risk if a child's personal information is used for unintended purposes.

Better Practice

Parental consent is required before personal information is collected or disclosed.

Worse Practice

Parental consent is not required before personal information is collected or disclosed.

Statutes & Regulations:

- COPPA: (A site directed to children is where the operator has actual knowledge the site is collecting information from children under the age of 13 and parental consent is required before any collection or use of information.) [597]
- COPPA: (A mixed audience site is where the site is directed to children, but does not target children as its "primary audience," but rather teens 13-to-18 years of age or adults. An operator of a mixed audience site is required to obtain age information from a user before collecting any information and if a user identifies themselves as a child under the age of 13, the operator must obtain parental consent before any information is collected.) [598]
- COPPA: (An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children.) [599]
- COPPA: (An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology and existing methods available to a parent to prove their identity.) [600]
- FERPA: (A school is prohibited from disclosing a student's "education record" or data to third parties without parental consent.) [601]
- FERPA: (A parent or eligible student is required to provide a signed and dated written consent before an educational institution discloses personally identifiable information from the student's records.) [602]
- GDPR: (In relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.) [603]

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

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

[599] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5.

[600] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(b)(i)-(iv).

[601] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30.

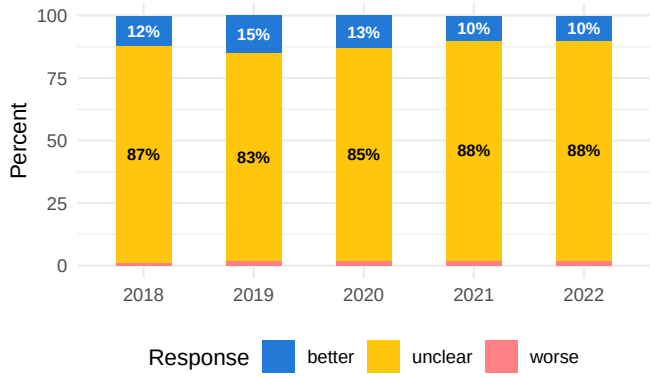
[602] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.30.

[603] General Data Protection Regulation (GDPR) 2016/679, Conditions Applicable to Child's Consent in Relation to Information Society Services, Art. 8(1).

11.3.2: Limit Consent

Do the policies clearly indicate whether or not a parent can consent to the collection and use of their child's personal information without also consenting to the disclosure of the information to third parties?

Figure 136: Limit Consent



The Limit Consent evaluation question indicates that parental consent is obtained for the collection and use of their child's or student's personal information with the product and consent is separate from any additional consent required for the disclosure of their child or student's information to third parties. A company should obtain parental consent for each particular purpose in which personal information is collected and used from children and obtain separate consent for any different purpose, such as disclosing a child's information to third parties for their own purposes.

Better Practice

Parental consent is limited with respect to third parties.

Worse Practice

Parental consent is not limited with respect to third parties.

Statutes & Regulations:

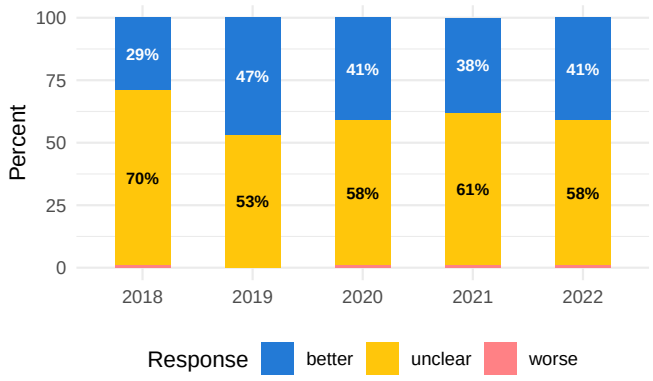
- COPPA: (An operator can not condition a child's participation in the service by sharing any collected information with third parties. A parent is required to have the ability to consent to the collection and use of their child's personal information without also consenting to the disclosure of the information to third parties.) [604]

[604] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(a)(2).

11.3.3: Withdraw Consent

Do the policies clearly indicate whether or not the company responds to a request from a parent or guardian to prevent further collection of their child's information?

Figure 137: Withdraw Consent



The Withdraw Consent evaluation question indicates that the company will prevent further collection and use of a child's personal information if requested from a parent or guardian. A company should respond to a verifiable request from a parent or guardian to opt out from the collection, use, or disclosure of their child's or student's personal information.

Better Practice

Parents can withdraw consent for the further collection of their child's information.

Worse Practice

Parents cannot withdraw consent for the further collection of their child's information.

Statutes & Regulations:

- COPPA: (An operator is required to provide a parent or guardian access to review, modify, or delete their children's information or prevent further collection of information.) [605]
- GDPR: (The controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: ... (c) the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.) [606]
- GDPR: (The controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: (d) the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.) [607]

[605] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(c); See also 16 C.F.R. Part 312.4(d)(3); 16 C.F.R. Part 312.6.

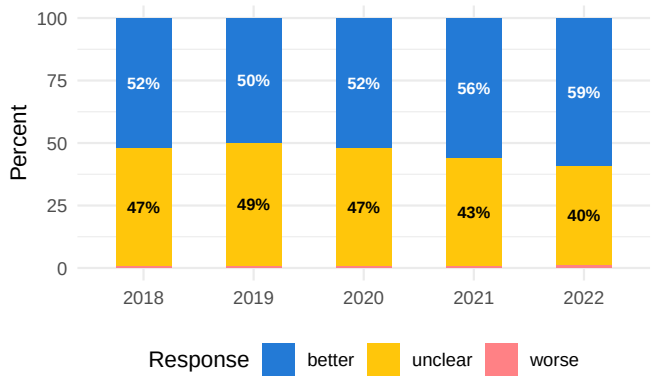
[606] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(2)(c).

[607] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(2)(d).

11.3.4: Delete Child-PII

Do the policies clearly indicate whether or not the company deletes personal information from a child under 13 years of age if collected without parental consent?

Figure 138: Delete Child-PII



The Delete Child-PII evaluation question indicates that the company will delete personal information from a child or student under 13 years of age if the information is collected without parental consent. A company should respond to any requests to delete personal information from the product if they receive a verifiable request that the information is from a particular user who is under the age of 13 and was collected without parental consent.

Better Practice

Children's personal information is deleted if collected without parental consent.

Worse Practice

Children's personal information is not deleted if collected without parental consent.

Statutes & Regulations:

- COPPA: (If the operator has not obtained parental consent after a reasonable time from the date of the information collection, or been given actual notice that information from a child under the age of 13 has been collected without parental consent, the operator must delete the information from its records.) [608]
- FERPA: (A parent or guardian can request the educational agency to access, modify, or delete their student's education records.) [609]

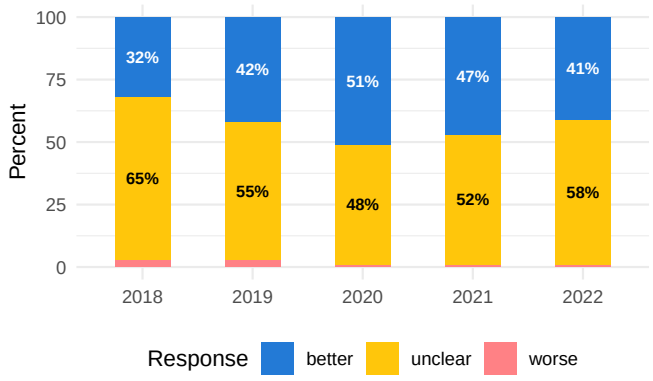
[608] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(1); See also 16 C.F.R. Part 312.6(c).

[609] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.10; See also 34 C.F.R. Part 99.20.

11.3.5: Consent Method

Do the policies clearly indicate whether or not the company provides notice to parents or guardians of the methods to provide verifiable parental consent?

Figure 139: Consent Method



The Consent Method evaluation question indicates the company's different methods available for parents or guardians to provide verifiable parental consent for their children's use of the product. A company should disclose to parents how they can provide parental consent such as creating a registered account with the product, creating a separate child profile, or using another COPPA-recognized method such as a consent form signed by the parent, a monetary transaction, a toll-free telephone number or videoconference, or verifying a parent's identity by checking a form of government-issued identification.

Better Practice

Parental consent notice and method for submission are provided.

Worse Practice

Parental consent notice and method for submission are not provided.

Statutes & Regulations:

- COPPA: (An operator is required to provide direct notice to parents describing what information is collected, how information is used, its disclosure practices and exceptions.) [610]
- COPPA: (Existing methods to obtain verifiable parental consent include: (i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan; (ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder; (iii) Having a parent call a toll-free telephone number staffed by trained personnel; (iv) Having a parent connect to trained personnel via video-conference; (v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete.) [611]
- COPPA: (If an operator does not "disclose" children's personal information, they may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email.) [612]

[610] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.4(b).

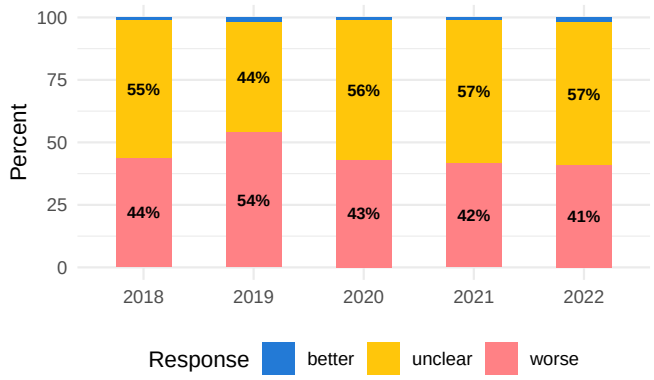
[611] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(b)(i)-(v).

[612] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(b)(vi).

11.3.6: School Consent

Do the policies clearly indicate whether or not responsibility or liability for obtaining verified parental consent is transferred to the school or district?

Figure 140: School Consent



The School Consent evaluation question indicates whether the responsibility for obtaining verified parental consent is transferred to the school or district. A company is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from students under 13 years of age. However, COPPA allows schools to act as an intermediary for parental consent in the process of collecting personal information from students, but this consent is limited to the educational context where the product is used, and where students' information is collected solely for the use and educational benefit of the school or district.

Better Practice

Parental consent obligations are not transferred to the school or district.

Worse Practice

Parental consent obligations are transferred to the school or district.

Statutes & Regulations:

- COPPA: (A vendor is required to provide a clear privacy policy about: (1) what information is collected, (2) how information is used, and (3) its disclosure practices of that information.) [613]
- COPPA: (An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children.) [614]

[613] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.3(a); See also 16 C.F.R. Part 312.4(d)(2).

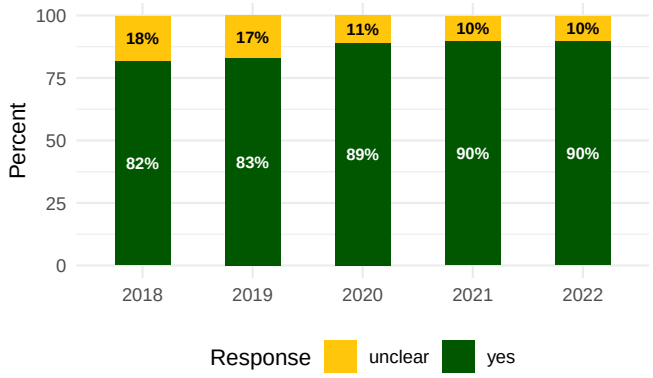
[614] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5.

Legal Requirements

11.4.1: Policy Jurisdiction

Do the policies clearly indicate the companys's legal jurisdiction that applies to the construction, interpretation, and enforcement of the policies?

Figure 141: Policy Jurisdiction



The Policy Jurisdiction evaluation question indicates the domestic state or foreign legal jurisdiction forum that applies to the enforcement of the company's policies. A company should provide a legal jurisdiction forum for the interpretation and enforcement of the policies that would be considered reasonably accessible by the majority of users of the product.

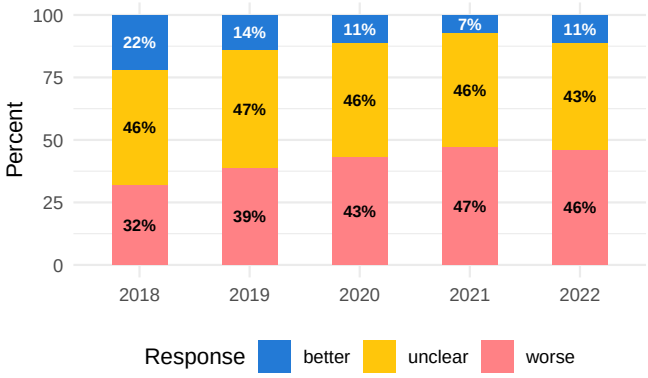
Transparent Practice

The legal jurisdiction that applies to the laws governing the policies is indicated.

11.4.2: Dispute Resolution

Do the policies clearly indicate whether or not the company requires a user to waive the right to a jury trial, or settle any disputes by Alternative Dispute Resolution (ADR)?

Figure 142: Dispute Resolution



The Dispute Resolution evaluation question indicates the company has a requirement that users must waive the right to a jury trial and settle any disputes by Alternative Dispute Resolution (ADR). A company should provide users with the opportunity to opt-out of the requirement that they must settle any disputes by Alternative Dispute Resolution (ADR) during account registration.

Better Practice

A user is not required to waive the right to a jury trial, or settle any disputes by arbitration.

Worse Practice

A user is required to waive the right to a jury trial, or settle any disputes by arbitration.

Statutes & Regulations:

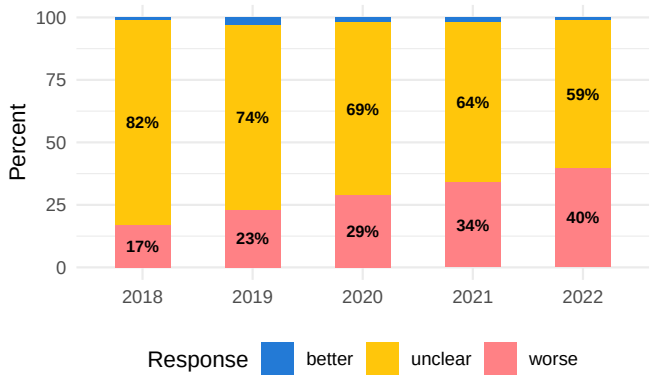
- DSA: (Recipients of the service, including individuals or entities that have submitted notices, shall be entitled to select any out-of-court dispute settlement body that has been certified in order to resolve disputes relating to those decisions, including complaints that have not been resolved by means of the internal complaint-handling system.) [615]

[615] Digital Services Act (Regulation (EU) 2022/2065), Out-of-court dispute settlement, Art. 21.

11.4.3: Class Waiver

Do the policies clearly indicate whether or not the company requires the user to waive their right to join a class action lawsuit?

Figure 143: Class Waiver



The Class Waiver evaluation question indicates whether the company has a requirement that users must waive any legal rights to join a class-action lawsuit in the event of a dispute. A company should provide users with the opportunity to opt out of the requirement that they waive the right to join a class-action lawsuit during account registration to preserve all their legal rights in the event of a dispute with the company.

Better Practice

A user is required to waive the right to join a class action lawsuit.

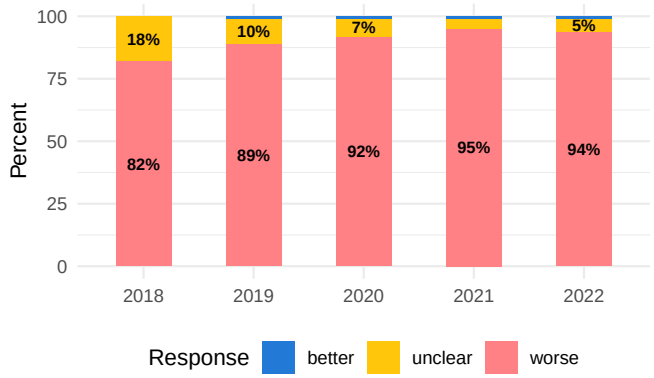
Worse Practice

A user is required to waive the right to join a class action lawsuit.

11.4.4: Law Enforcement

Do the policies clearly indicate whether or not the company can use or disclose a user's data under a requirement of applicable law to comply with a legal process, to respond to governmental requests, to enforce their own policies, for assistance in fraud detection and prevention, or to protect the rights, privacy, safety or property of the company, its users, or others?

Figure 144: Law Enforcement



The Law Enforcement evaluation question indicates that a user's information may be shared with government, private, or legal authorities to protect the company or to protect the health, privacy, or safety of the product's users. A company should not disclose a user's information to government, private, or legal authorities without due process.

Better Practice

A company will not disclose personal information to law enforcement.

Worse Practice

A company will disclose personal information to law enforcement.

Statutes & Regulations:

- COPPA: (An operator is prohibited from sharing a child's information to third parties except in limited circumstances to ensure legal and regulatory compliance; respond to or participate in a judicial process; or to protect the safety of a child; or provide information to law enforcement agencies.) [616]
- FERPA: (An operator is prohibited from sharing a student's information to third parties except in limited circumstances to ensure legal and regulatory compliance; respond to or participate in a judicial process; in connection with a health or safety emergency, or violation of any Federal, State, or local law.) [617]
- SOPIPA: (An operator is prohibited from sharing student information to third parties except in limited circumstances to ensure legal and regulatory compliance; respond to or participate in a judicial process; or to protect the safety of users, others, or the security of the site.) [618]
- CalECPA: (Prohibits a government entity from compelling the production of or access to electronic communication information or electronic device information, without a search warrant, wiretap order, order for electronic reader records, or subpoena issued under specified conditions, except for emergency situations.) [619]
- CCPA: (A business shall not be restricted to comply with federal, state, or local laws or comply with a court order or subpoena to provide information. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities. Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law. Cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury and exercise or defend legal claims.) [620]
- DSA: (Where a provider of hosting services becomes aware of any information giving rise to a suspicion that a criminal offense involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place, it shall promptly inform the law enforcement or judicial authorities of the Member State or Member States concerned of its suspicion and provide all relevant information available.) [621]

[616] Children's Online Privacy Protection Act (COPPA), 16 C.F.R. Part 312.5(c)(5)-(6).

[617] Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. Part 99.31(5),(9),(10),(13)-(16); See also 34 C.F.R. Part 99.36

[618] Student Online Personal Information Protection Act (SOPIPA), Cal. B.&P. Code § 22584(b)(4)(B)-(C),(k).

[619] California Electronic Communications Privacy Act, Cal. Pen. Code § 1546-1546.4.

[620] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.145(a)(1)-(5).

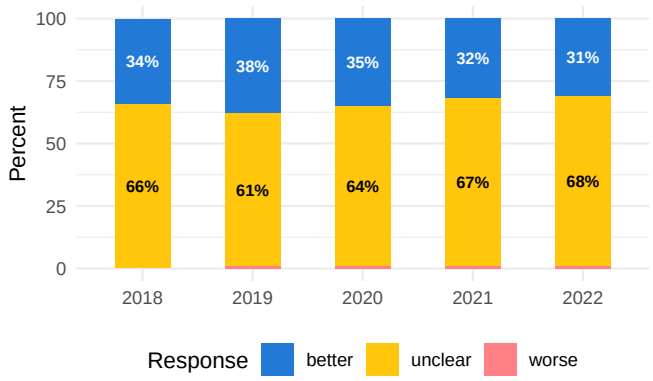
[621] Digital Services Act (Regulation (EU) 2022/2065), Notification of suspicions of criminal offenses, Art. 18.

Certification

11.5.1: Privacy Badge

Do the policies clearly indicate whether or not the company has signed any privacy pledges or received any other privacy certifications?

Figure 145: Privacy Badge



The Privacy Badge evaluation question indicates that the company has made a commitment to a third-party privacy certification, badge, codes of conduct, or principles of a privacy pledge. A company that has earned a certification toward their better privacy-protecting practices – and has demonstrated that compliance to its users – can create stronger trust and safety with the users of its product and differentiate themselves from their competitors on privacy.

Better Practice

The company has signed a privacy pledge or received a privacy certification.

Worse Practice

The company has not signed a privacy pledge or received a privacy certification.

Statutes & Regulations:

- GDPR: (Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.) [622]

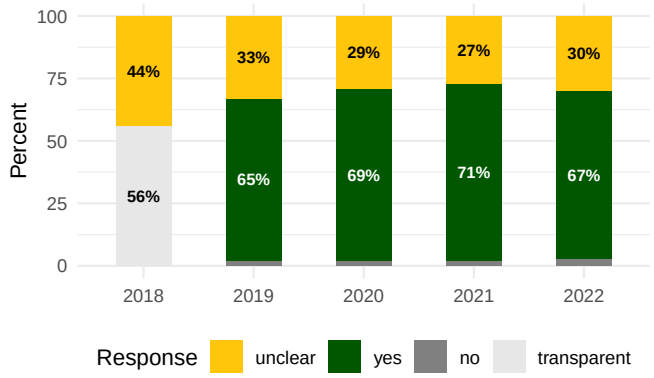
[622] General Data Protection Regulation (GDPR) 2016/679, Responsibility of the Controller, Art. 24(3).

International Laws

11.6.1: Jurisdictional Transfer

Do the policies clearly indicate whether or not a user's data are subject to International data transfer or jurisdiction laws, such as a privacy shield or a safe harbor framework that protects the cross-border transfer of a user's data?

Figure 146: Jurisdictional Transfer



The Jurisdictional Transfer evaluation question indicates whether or not a user's data are subject to International data transfer or jurisdiction laws such as the GDPR. A company with users in other countries should disclose how its data practices are applied to different countries and have suitable safeguards in place relating to the transfer of users' data between countries.

Qualitative Status: Complex

The qualitative nature of this question is complex and requires additional context outside the scope of our privacy evaluation to determine the qualitative nature of this practice.

Statutes & Regulations:

- GDPR: (The EU General Data Protection Regulation (GDPR) 2016/679 replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy, and to reshape the way organizations across the region approach data privacy.) [623]
- GDPR: (This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.) [624]
- GDPR: (This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union.) [625]
- GDPR: (This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.) [626]
- GDPR: ("binding corporate rules" means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.) [627]
- GDPR: ("cross-border processing" means either: (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.) [628]
- GDPR: (Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: ... (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.) [629]
- GDPR: (Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: ... (f) where applicable, that the controller intends to transfer personal data to a recipient in a

[623] General Data Protection Regulation (GDPR) 2016/679.
[624] General Data Protection Regulation (GDPR) 2016/679, Territorial Scope, Art. 3(1).
[625] General Data Protection Regulation (GDPR) 2016/679, Territorial Scope, Art. 3(2)(a)-(b).
[626] General Data Protection Regulation (GDPR) 2016/679, Territorial Scope, Art. 3(3).
[627] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(20).
[628] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(23)(a)-(b).
[629] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(1)(f).

third country or international organisation and the existence or absence of an adequacy decision by the Commission, or ... reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.) [630]

- GDPR: (Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.) [631]
- GDPR: (Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.) [632]
- GDPR: (A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.) [633]
- GDPR: (Where jurisdiction applies, the controller or the processor shall designate in writing a representative in the Union.) [634]
- GDPR: (Controller or processor obligation shall not apply to: (a) processing which is occasional, does not include, on a large scale, processing of special categories of data ... or processing of personal data relating to criminal convictions and offenses ... and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing.) [635]
- GDPR: (The representative shall be established in one of those Member States where the data subjects are and whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored.) [636]
- GDPR: (The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.) [637]

[630] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(1)(f).

[631] General Data Protection Regulation (GDPR) 2016/679, Right of access by the data subject, Art. 15(2).

[632] General Data Protection Regulation (GDPR) 2016/679, General principle for transfers, Art. 44.

[633] General Data Protection Regulation (GDPR) 2016/679, Transfers on the basis of an adequacy decision, Art. 45(1).

[634] General Data Protection Regulation (GDPR) 2016/679, Representatives of controllers or processors not established in the Union, Art. 27(1).

[635] General Data Protection Regulation (GDPR) 2016/679, Representatives of controllers or processors not established in the Union, Art. 27(2).

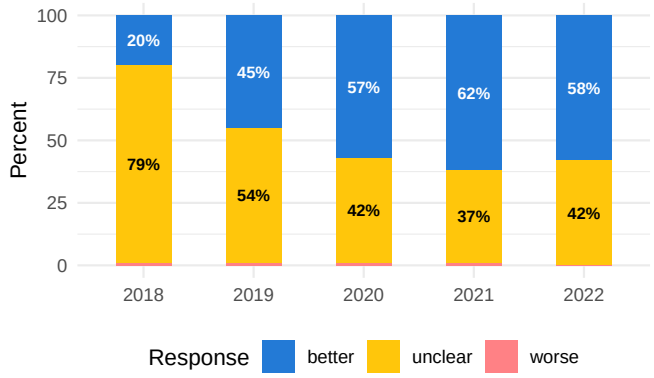
[636] General Data Protection Regulation (GDPR) 2016/679, Representatives of controllers or processors not established in the Union, Art. 27(3).

[637] General Data Protection Regulation (GDPR) 2016/679, Representatives of controllers or processors not established in the Union, Art. 27(4).

11.6.2: GDPR Role

Do the policies clearly indicate whether or not the company is categorized as a Data Controller or a Data Processor, and whether it has identified a Data Protection Officer (DPO) for the purposes of GDPR compliance?

Figure 147: GDPR Role



The GDPR Role evaluation question indicates whether the company is categorized as a data controller or a data processor, and if a Data Protection Officer (DPO) can be contacted. A company should disclose the type of relationship it has with users of its product as either a controller or processor. A company should also provide information to users on how to contact the company's data protection officer to answer privacy-related questions about the product.

Better Practice

The company has indicated it is a Data Controller or Data Processor.

Worse Practice

The company has not indicated it is a Data Controller or Data Processor.

Statutes & Regulations:

- GDPR: ("controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.) [638]
- GDPR: (Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.) [639]
- GDPR: (This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.) [640]
- GDPR: ("processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.) [641]
- GDPR: ("processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.) [642]
- GDPR: (Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: ... (b) the contact details of the data protection officer, where applicable.) [643]
- GDPR: (Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: ... (b) the contact details of the data protection officer, where applicable.) [644]
- GDPR: (The controller and the processor shall designate a data protection officer in any case where: ... (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.) [645]
- CCPA: ("Processing" means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.) [646]

[638] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(7).
[639] General Data Protection Regulation (GDPR) 2016/679, Records of Processing Activities, Art. 30(1)-(4).
[640] General Data Protection Regulation (GDPR) 2016/679, Material Scope, Art. 2(1).
[641] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(2).
[642] General Data Protection Regulation (GDPR) 2016/679, Definitions, Art. 4(8).
[643] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data are collected from the data subject, Art. 13(1)(b).
[644] General Data Protection Regulation (GDPR) 2016/679, Information to be provided where personal data have not been obtained from the data subject, Art. 14(1)(b).
[645] General Data Protection Regulation (GDPR) 2016/679, Designation of the data protection officer, Art. 37(1)(b).
[646] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(y).

Appendix

Basic Questions

Policy Available, Effective Date, Children Intended, Students Intended, Collect PII, PII Categories, Collection Limitation, Data Shared, Third-Party Marketing, Sell Data, Third-Party Limits, User Submission, Access Data, Data Modification, User Deletion, Deletion Process, Transfer Data, Transit Encryption, Storage Encryption, Breach Notice, Safe Interactions, Unsafe Interactions, Visible Data, Contextual Ads, Personalised Ads, Third-Party Tracking, Track Users, Ad Profile, Company's Marketing, Parental Consent

Rating Questions

Policy Available, Effective Date, Sell Data, Third-Party Marketing, Personalised Ads, Third-Party Tracking, Track Users, Ad Profile

Concern Questions

Data Collection

Evaluating data collection takes into consideration best practices of limiting the type and amount of personal information collected from a user to only the information needed to provide the application or service.

What data does it collect?

Collect PII, PII Categories, Collection Limitation, Geolocation Data, Health Data, Behavioral Data, Sensitive Data, Usage Data, Collection Consent, Third-Party Collection

Data Sharing

Evaluating data sharing takes into consideration best practices that protect the disclosure of a user's personal information to third parties.

What data does it share?

Data Shared, Data Categories, Sharing Purpose, Related Third-Party, Third-Party Analytics, Third-Party Research, Third-Party Providers, Third-Party Roles, Third-Party Login, Third-Party Limits

Data Security

Evaluating data security takes into consideration best practices that protect the integrity and confidentiality of a user's data.

How does it secure data?

Verify Identity, Account Required, Managed Account, Multi-Factor Protection, Security Agreement, Reasonable Security, Physical Access, Transit Encryption, Storage Encryption, Breach Notice

Data Rights

Evaluating data rights takes into consideration best practices of providing users with the ability to review, access, modify, delete, and export their personal information and content.

What rights do I have to the data?

User Submission, Data Ownership, Access Data, Data Modification, Retention Policy, Deletion Process, Account Deletion, Deletion Purpose, Restrict Access, User Export

Data Sold

Evaluating data selling takes into consideration best practices of not sharing, renting, or selling a user's personal information to third parties for financial gain.

Is the data sold?

Sell Data, Opt-Out Consent, Transfer Data, Transfer Notice, Transfer Deletion, Transfer Limits, Data De-identified, De-identified Process, Third-Party Research, Combination Limits

Data Safety

Evaluating safety takes into consideration best practices that protect a user's physical and emotional health.

How safe is this product?

Safe Interactions, Unsafe Interactions, Share Profile, Visible Data, Control Visibility, Monitor Content, Filter Content, Moderating Interactions, Log Interactions, Report Abuse

Ads & Tracking

Evaluating ads and tracking takes into consideration best practices of not using a user's personal information for any third-party marketing, behavioral advertising, tracking, or profile generation purposes.

Are there advertisements or tracking?

Third-Party Marketing, Contextual Ads, Personalised Ads, Third-Party Tracking, Track Users, Ad Profile, Company's Marketing, Third-Party Promotions, Unsubscribe Ads, Unsubscribe Marketing

Parental Consent

Evaluating parental consent takes into consideration best practices of protecting children under 13 years of age by requiring a parent's or guardian's verifiable consent before the collection, use, or disclosure of a child's personal information to an application or service.

Can I provide parental consent?

Children Intended, Child Data, Parents Intended, Actual Knowledge, Children's Privacy, Parental Consent, Limit Consent, Withdraw Consent, Delete Child-PII, Consent Method

School Purpose

Evaluating school purpose takes into consideration best practices of companies that collect personal information from students or teachers in K-12 and the legal obligations for the privacy and security of that information.

Is the product intended for school?

Students Intended, Student Data, Teachers Intended, School Purpose, Education Records, School Contract, School Official, School Consent

Individual Control

Responsible data use practices limit how personal information is used to only what's necessary to provide the application or service and user controls allow data practices to change.

Can I control the use of my data?

Privacy Settings, Purpose Limitation, Data Purpose, Company Combination, Combination Type, Context Notice, Context Consent, Complaint Notice, Disclosure Request, Disclosure Notice

Statutes & Regulations

California Online Privacy Protection Act (CalOPPA)

Effective Date, Change Notice, Method Notice, Review Changes, Effective Changes, Services Include, Company Contact, Collect PII, PII Categories, Geolocation Data, Usage Data, Exclude Sharing, Data Obtained, Authorized Access, Third-Party Collection, Related Third-Party, Access Data, Review Data, Data Modification, Modification Process, User Deletion, Third-Party Tracking, Track Users, DoNotTrack Response, DoNotTrack Description

California "Shine the Light" (ShineTheLight)

Third-Party Marketing, Opt-Out Consent, Disclosure Request, Unsubscribe Marketing

Protection of Pupil Rights Act (PPRA)

Teachers Intended, Third-Party Research, Third-Party Promotions

California Data Breach Notification Requirements (DataBreach)

Reasonable Security, Transit Encryption, Storage Encryption, Breach Notice

California Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA)

Legacy Contact

California Privacy of Pupil Records (AB 1584)

Third-party Deletion, Purpose Limitation, Data Ownership, Review Data, Modification Process, Deletion Purpose, User Export, Security Agreement, Reasonable Security, Physical Access, Data Jurisdiction, Breach Notice, Personalised Ads, School Contract, School Official

California Privacy of Pupil Records (CalPPR)

Students Intended, Third-Party Research, Login Collection, Data De-identified, Review Data, Modification Process, Deletion Process

California Privacy Rights for Minors in the Digital World (CalPRMDW)

Teens Intended, Third-Party Marketing, User Deletion, Block Content, Safe Tools, Track Users, Ad Profile, Filter Ads, Company's Marketing

California Electronic Commerce Act (CalECA)

Company Contact

California Electronic Communications Privacy Act (CalECPA)

Disclosure Notice, Law Enforcement

Children's Internet Protection Act (CIPA)

Outbound Links, Block Content, Safe Tools, Filter Ads

Digital Millennium Copyright Act (DMCA)

Complaint Notice

Copyright Act of 1976 (Copyright)

Data Ownership, Copyright License

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM)

Unsubscribe Marketing

The Communications Decency Act of 1996 (CDA)

Complaint Notice, Monitor Content, Block Content, Safe Tools

Children's Online Privacy Protection Act (COPPA)

Company Contact, Children Intended, Teens Intended, Adults Intended, Parents Intended, Collect PII, PII Categories, Geolocation Data, Health Data, Behavioral Data, Usage Data, Child Data, Collection Limitation, Data Shared, Data Categories, Sharing Purpose, Third-Party Analytics, Third-Party Research, Third-Party Marketing, Sell Data, Third-Party Providers, Third-Party Roles, Company Combination, Third-Party Combination, Third-Party Login, Data De-identified, De-identified Process, Third-Party Limits, Combination Limits, Purpose Limitation, Combination Type, Collection Consent, Access Data, Restrict Access, Review Data, Maintain Accuracy, Modification Process, Deletion Purpose, Account Deletion, Deletion Process, Transfer Data, Transfer Limits, Verify Identity, Security Agreement, Reasonable Security, Data Jurisdiction, Safe Interactions, Unsafe Interactions, Share Profile, Visible Data, Filter Content, Moderating Interactions, Contextual Ads, Personalised Ads, Third-Party Tracking, Track Users, Ad Profile, Company's Marketing, Third-Party Promotions, Unsubscribe Ads, Actual Knowledge, Children's Privacy, Child-Prohibited Account, Parental Consent, Limit Consent, Withdraw Consent, Delete Child-PII, Consent Method, School Consent, Law Enforcement

Family Educational Rights and Privacy Act (FERPA)

Students Intended, Teachers Intended, Collect PII, Geolocation Data, Health Data, Behavioral Data, Usage Data, Student Data, Data Shared, Third-Party Research, Data De-identified, De-identified Process, Third-Party Limits, Disclosure Request, Disclosure Notice, Restrict Access, Review Data, Modification Process, Retention Exception, Account Deletion, Deletion Process, Verify Identity, Security Agreement, Reasonable Security, Track Users, School Purpose, Education Records, School Contract, School Official, Parental Consent, Delete Child-PII, Law Enforcement

Student Online Personal Information Protection Act (SOPIPA)

Students Intended, Teachers Intended, Geolocation Data, Health Data, Usage Data, Student Data, Data Shared, Sharing Purpose, Third-Party Analytics, Third-Party Research, Sell Data, Third-Party Providers, Third-Party Roles, Third-Party Combination, Third-Party Login, Data De-identified, De-identified Process, Third-Party Limits, Purpose Limitation, Account Deletion, Deletion Process, User Export, Transfer Data, Transfer Limits, Security Agreement, Reasonable Security, Data Jurisdiction, Personalised Ads, Third-Party Tracking, Track Users, Ad Profile, School Purpose, Law Enforcement

Early Learning Personal Information Protection Act (ELPIPA)

Students Intended, Teachers Intended, Student Data, School Purpose

General Data Protection Regulation (GDPR)

Company Contact, Privacy Summary, Preferred Language, Children Intended, Teens Intended, Adults Intended, Collect PII, PII Categories, Geolocation Data, Health Data, Behavioral Data, Sensitive Data, Usage Data, Collection Limitation, Data Shared, Sharing Purpose, Third-Party Analytics, Exclude Sharing, Sell Data, Data Obtained, Third-Party Providers, Related Third-Party, Company Combination, Data De-identified, De-identified Process, Third-Party Limits, Purpose Limitation, Data Purpose, Context Notice, Context Consent, Collection Consent, Complaint Notice, Opt-Out Consent, Disclosure Request, Disclosure Notice, Access Data, Restrict Access, Maintain Accuracy, Data Modification, Modification Process, Modification Time, Retention Policy, Retention Exception, Deletion Purpose, User Deletion, Deletion Time, User Export, Transfer Limits, Verify Identity, Security Agreement, Reasonable Security, Transit Encryption, Storage Encryption, Data Jurisdiction, Breach Notice, Audit Practices, Ad Profile, Unsubscribe Marketing, School Contract, Parental Consent, Withdraw Consent, Privacy Badge, Jurisdictional Transfer, GDPR Role

The California Consumer Privacy Act (CCPA)

Effective Changes, Adults Intended, Collect PII, PII Categories, Geolocation Data, Health Data, Behavioral Data, Sensitive Data, Usage Data, Collection Limitation, Data Shared, Data Categories, Sharing Purpose, Third-Party Analytics, Third-Party Research, Third-Party Marketing, Sell Data, Data Obtained, Third-party Deletion, Third-Party Providers, Third-Party Roles, Related Third-Party, Third-Party Policy, Third-Party Combination, Third-Party Login, Data De-identified, De-identified Process, Third-Party Limits, Combination Limits, Purpose Limitation, Data Purpose, Context Notice, Collection Consent, Privacy Settings, Opt-Out Consent, Disclosure Request, Review Data, Data Modification, Modification Process, Modification Time, Retention Policy, Retention Exception, Deletion Purpose, Account Deletion, User Deletion, Deletion Process, Deletion Time, User Export, Transfer Data, Verify Identity, Account Required, Reasonable Security, Physical Access, Transit Encryption, Storage Encryption, Breach Notice, Service Messages, Contextual Ads, Personalised Ads, Third-Party Tracking, Track Users, Ad Profile, Company's Marketing, DoNotTrack Response, Actual Knowledge, Education Records, Law Enforcement, GDPR Role

The California Age-Appropriate Design Code Act (CAADCA)

Children Intended, Teens Intended, Geolocation Data, Behavioral Data, Child Data, Collection Limitation, Sell Data, Purpose Limitation, Community Guidelines, Privacy Settings, Opt-Out Consent, Review Data, Modification Process, Retention Policy, Deletion Process, Managed Account, Audit Practices, Control Visibility, Report Abuse, Track Users, Ad Profile, Filter Ads, Third-Party Promotions, Actual Knowledge, Children's Privacy

The Digital Services Act (DSA)

Change Notice, Company Contact, Preferred Language, Children Intended, Complaint Notice, Privacy Settings, Opt-Out Consent, Monitor Content, Report Abuse, Contextual Ads, Personalised Ads, Ad Profile, Actual Knowledge, Children's Privacy, Dispute Resolution, Law Enforcement

Telecommunications Act (Telecom Act)

PII Categories, Geolocation Data, Usage Data, Data De-identified, Purpose Limitation, Company's Marketing