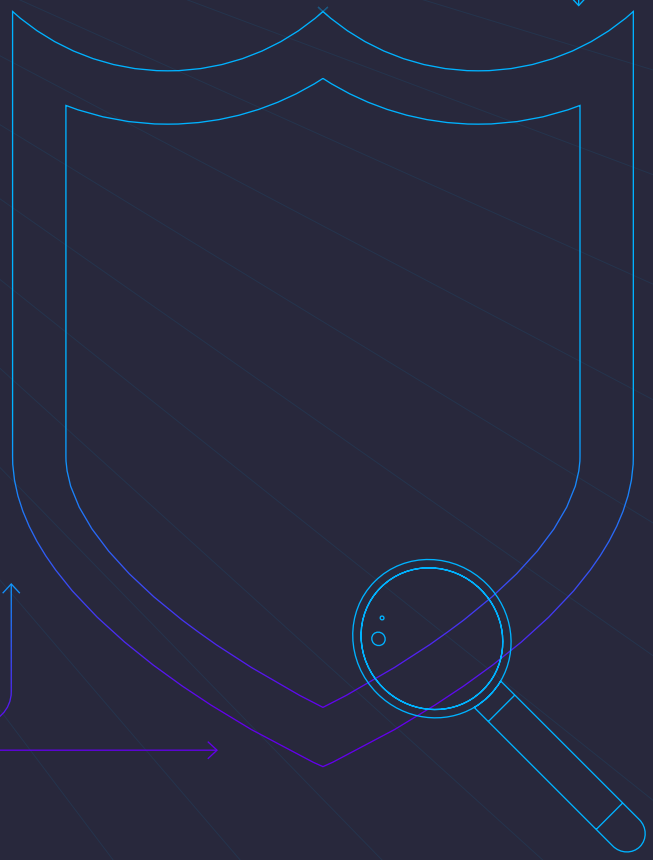
Center for Industry Self-Regulation

Self-Regulation Incubator:
TeenAge Privacy Program

# The 2.0 Roadmap for Considering Teen Privacy & Safety



# Table of Contents

**Executive Summary** . . . . . **3**
Background . . . . . 4
**Guiding Considerations** . . . . . **5**
**Signposts for Teen Privacy & Safety** . . . . . **6**
Age Assurance Practices . . . . . 7
Collection of Teen Data . . . . . 8
Use & Retention of Teen Data . . . . . 11
Sharing of Teen Data . . . . . 16
Social Features . . . . . 17
In-App Purchases . . . . . 19
Parental Tools . . . . . 21
Research Practices . . . . . 22
**Appendix** . . . . . **23**

# Executive Summary

A wave of legislative and regulatory activity in the teenage data privacy space has encompassed the globe in recent years, more recently grounded in new state consumer and teenage data privacy laws taking effect in the United States. While U.S. federal privacy legislation was introduced to uphold stronger data privacy protections when processing personal information of the 13 to 17 teenage user group, no critical action has fully formed and passed out of Congress, leaving further opportunity for precedent to be set by the Federal Trade Commission (FTC) in its enforcement action and for states to take on a more critical role in determining best practices. Thus, the ever-changing, self-fulfilling state patchwork results in confusion regarding what the rules of the road are, for regulators, consumers, and businesses alike. Here, self-regulation plays a key role, as industry accountability agents can set the stage for a more uniform set of obligations that take the patchwork into consideration but also seeks to understand and level-set practical industry considerations that won't chill innovation.

For BBB National Programs, developing an updated TAPP Roadmap involved two important sets of considerations. First, there are best practices and lessons learned from the host of FTC regulatory enforcement activities setting precedent about how companies are misusing teen and children's personal information. Second, in lieu of federal laws governing teen and minors' privacy (extending beyond requirements in the Children's Online Privacy Protection Act), states have set new benchmarks for teen privacy.

In addition to privacy considerations, legislation to protect minors from online harms has also touched on issues of deception, content moderation, and safety. The FTC enforcement has followed this line of thinking.

The primary considerations states are developing to combat online harms to minors fall into two camps: (1) areas of general agreement and (2) tailored approaches, where states diverge.

**State consumer privacy laws and social media/online safety laws seem to take common approaches to:**

- Providing minors with consumer rights regarding access to their data (access, deletion, ability to consent and withdraw consent and delete their accounts),
- Limiting design features that contribute to compulsive usage, and
- Including obligations for companies to have a duty of care, data minimization, and purpose specifications toward minors' data, in addition to expectations regarding data security.

**Differing state perspectives exist regarding:**

- The age threshold of what is considered a "teen,"
- Requirements (if any) for parental consent and parental access to teen online data,

- Moderation of user-generated content,
- Features that facilitate interactions between teen users and strangers/adults,
- Use of teen data in algorithmic systems for content delivery, profiling, and decision making,
- The use of geolocation data,Age assurance requirements,
- Advertising requirements for the process of minors' data, and
- Requirements regarding impact assessments and whether they are mandatory.

# Background

The TAPP Roadmap was developed in 2022 by a diverse group of U.S. businesses to create a self-regulatory approach to teenage privacy and data rights. In 2023, the TAPP framework was updated to align the Roadmap's considerations with new state laws and set a minimum baseline for what companies should be obligated to do when processing teenage personal information.

For purposes of this document, "teenagers" and "teens" means consumers aged 13 to 17, inclusive. This document is grounded in the reasoning that even as data privacy and safety practices that work for adult consumers provide a firm foundation for teens, they simultaneously run the risk of being insufficient to respond to the unique needs of teens.

The teen stage of cognitive and social development means that the risks and harms implicit in the use of digital products and services may differ in both kind and degree for teen users. That is, privacy and other harms that affect adults may be more impactful to teens, while additional harms may be unique to this demographic (see Appendix: Background Research on Teen-Specific Privacy Harms).

To assist any businesses that wish to engage proactively with teen consumers, this document maps the broad spectrum of potential harms impacting teens onto a concrete set of operational considerations. A dedicated process for considering the unique needs of certain consumer groups, such as teens, is an important step in any design and development cycle. An organization of any size can use this Roadmap to help address the privacy, autonomy, and safety of teens.

# Guiding Considerations

- Fostering teen awareness of data privacy.
- Encouraging responsible processing of teen data.
- Building guardrails for teen interactions with others through digital systems.
- Reflecting on appropriate content for teens.

# Signposts for Teen Privacy & Safety

- Age Assurance Practices
- Collection of Teen Data
- Use & Retention of Teen Data
- Sharing of Teen Data
- Social Features
- In-App Purchases
- Parental Tools
- Research Practices

# Age Assurance Practices

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Determining the applicable user base – and the age of users on the platform;*<br><br>*And/or implementing age assurance technologies (i.e. age estimation/age verification systems)* | Are there circumstances where your organization would have knowledge a user is a minor - on the basis of appropriate due diligence?<br><br>What level of certainty do you have about a user's age given the potential risks of the product, service, or features to its users?<br><br>What is the appropriate age assurance method to determine user base, given the risks I have identified?<br><br>How can I ensure data collected for age assurance is not used for any other purpose? | » Due diligence to assess whether a minor is using the service could include: relying on competent and reliable empirical evidence and taking into account the totality of the circumstances, such as available tech and reasonable care involved.<br><br>» Comply with applicable state or federal laws where they proscribe specific age assurance requirements or methodologies.<br><br>» For services that are known to contain risks to minors, establish the age of consumers/account holders, and apply protective default privacy and safety settings to known teens.<br><br>*Prevent secondary uses of data collected for age assurance and only retain age assurance data for a reasonable period of time to perform verification or estimation, unless otherwise required to retain by law.<br><br>Determine whether feasible*:<br><br>» Even if not otherwise required by law, adopt appropriate assurance methodologies to establish the age of the user with a reasonable level of certainty.<br><br>*AADC preliminary injunction places the required nature of this into question, but it does not deter the best practice. | » Inappropriate treatment of teen users as adults<br><br>» Inappropriate content displayed to teen users<br><br>» Violating data minimization, purpose specification, and duty of reasonable care principles as found in global privacy regulations |

# Collection of Teen Data

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Obtaining consent prior to collection, sharing, or sale of teen personal information* | Do you review the types of data you collect from teenage users, specifically?<br><br>Are teens provided clear, meaningful, and prominent notice and consent – namely with an explanation of why they are to consent?<br><br>Are teens actively consenting to the choice to opt-in their personal information to the site, product, or service? | » Ensure the teen has provided affirmative opt-in consent (and just as easily understands the ability to withdraw consent) wherever possible.<br>» Implement clear disclosures and fine-tuned controls, including consent mechanisms that streamline the process to obtain consent).<br>» Avoid the use of manipulative, burdensome, or unduly suggestive design elements (including dark patterns) when obtaining opt-in consent from teenage users or when communicating to teenage users about privacy settings.<br>» Provide teenage users the ability to revoke consent at any time through a method as easy-to-use as the method consent was given. Provide an easy-to-understand notice of the ability to revoke consent to a teenage user at the top of any privacy settings page accessible to the teenage user.<br>» Incorporate parental involvement for opt-in consent for higher-risk situations, or where appropriate (e.g., AR social media law). | » Violating a teen's (and family's) privacy by sharing sensitive teen personal information without appropriate consent<br>» Lack of transparency to consumers about the data collection, sharing, or sale occurring and what options they have to exercise their rights and to consent or withdraw consent<br>» Potential violation of COPPA, if data sets are mixed across age groups from under 13 and over 13 users without obtaining appropriate consent<br>» May be considered a potential "data breach" when sharing teen personal information with third parties without consumer's consent (per FTC/other regulators) |
| *Purpose specification; Ensuring data minimization and duty of care* | Do you clearly specify the purpose(s) for collecting teen personal information, including primary and secondary purposes? | » Specify the purpose of the collection, sharing, or sale, and avoid the use of personal information of the teen for any reason other than the reason for which the personal information was collected, unless the online platform can demonstrate a compelling reason that the use of the personal information does not pose a substantial harm or privacy risk to children. | » Lack of transparency about the data collection, sharing, or sale occurring<br>» Unexpected uses of data<br>» Normalization of over- collection of data<br>» Increased risks of data breach |

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Purpose specification; Ensuring data minimization and duty of care* | Do you limit the collection of teen information to what is necessary to fulfill the online product or service? | » Where appropriate, ensure the purpose specification is acceptable and comprehensible by teen-age users.<br>» Use default settings to minimize data collection, sharing, or sale to what is necessary for the delivery of the product or service the consumer expects.*<br>* AADC preliminary injunction places the required nature of this into question, but many other existing laws place importance on the data minimization and purpose specification principles. | » Creation of a larger digital footprint outside of a teen's control or awareness<br>» Unauthorized collection of personal information<br>» Unauthorized sharing of personal information with services providers or other third parties<br>» Unnecessary collection of personal information |
| *Collection/sharing for interest-based advertising* | Do you collect information on interests or behavior for the purpose of targeting ads?<br>Are teen users made aware that their information will be used for targeting ads, potentially across different sites or devices? | » Obtain opt-in consent before engaging in behavioral advertising to known teens (or in some states, where teens are likely to access the product or service), and/or limit purpose of collection to contextual advertising.<br>» Ensure opt-in consent for targeted advertising involves the parent, if and where appropriate (e.g., Texas SCOPE Act).<br>» At the time of obtaining opt-in consent, provide conspicuous notice that targeted ads based on information collected from teen users may be shown to the teen user across different sites or devices they use.<br>» Ensure consumer choice mechanism per the Digital Advertising Alliance's advertising standards so the user (or parent/guardian) can opt out and understands options for revoking consent.<br>» At the time of obtaining opt-in consent, provide conspicuous notice and point to external resources, where appropriate, that explain the tracking technologies (such as cookies) used to facilitate the advertising so that it is plain language and understandable to a teen audience. | » Unauthorized collection of personal information<br>» Unauthorized sharing of personal information with service providers or other third parties<br>» Unnecessary collection of personal information<br>» Increased risks of data breach |
| *Content in interest-based or targeted advertising and profiling by age* | Do you collect information that could be considered especially sensitive or harmful to teen demographics? | » Avoid targeting content to teens using a single criterion that could be especially sensitive to teens or amplify existing insecurities (e.g., body odor, hair loss, weight).<br>» Supplement messaging/advertising with content that counteracts the potential negative impact of the targeting. | » Hypertargeting<br>» Amplifying interests or insecurities in a way that intensifies harmful thoughts or behaviors |

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Content in interest-based or targeted advertising and profiling by age* | | » For U.S. and U.K. audiences, consider that sensitivities may be specific to age groups as laid out in global regulations: 13-15 (early teens), 16-17 (approaching adulthood). | |
| *Allowing users to post paid for or branded content without clear disclosures* | Do you establish sufficient policies, tools, and visual markers to make teen-age users aware when content is an advertisement? | » Don't blur advertising and other content. Adopting policies that clearly outline when content on your services constitutes an advertisement.<br>» Make policies on advertising easily accessible and easy to understand for all users and creators.<br>» Require content creators to disclose when content or messaging is an advertisement.<br>» Provide tools to content creators, such as flags or visual notices, to indicate when content or messaging is paid for by a brand. | » Deception/exploiting parasocial relationships |
| *Collection/sharing of teen's precise geolocation information* | Is precise geolocation information collection off by default for known teen users?<br><br>What guardrails exist for all other geolocation data (as opposed to precise geolocation data)?<br><br>Are there clear disclosures of what user action triggers the collection of precise geolocation information? | » Set the default to not collect precise geolocation data unless opted in or enabled by a verified parent or guardian, or unless strictly necessary for the participant to provide a product, service, or feature requested by the teenage user.<br>(Note: Some states like CT now prohibit the collection of all precise geolocation of minors (even with VPC or if it is strictly necessary to operate product or service).)<br>» Provide clear, up-front, opt-in disclosures.<br>» If location information is embedded in metadata for a teenage user's file upload (i.e., photos and videos), remove embedded location information as part of the upload process.<br>» Provide an obvious, in-application signal to the teen user that indicates when precise geolocation information is being collected.<br>» Serve routine reminders of ongoing collection of precise geolocation data (both in-context reminders and through other media (e.g., email). | » Unnecessary collection of personal information<br>» Potential safety harms include identification by external, bad actors which could lead to abduction, custody issues, stalking and harassment<br>» Potential for data breach if data is sharing without appropriate consent is obtained |

# Use & Retention of Teen Data

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Providing prominent, accessible, and responsive tools to help children (or if applicable their parents or guardians) exercise their privacy rights and report concerns* | Can the teen (or their parent or guardian) request access to their personal information on the digital service or site?<br><br>Does the teen (or their parent or guardian) have the right to request to unpublish information (in particular, when social media is concerned)?<br><br>Does the teen (or their parent or guardian) have the right to request their data be deleted within a commercially reasonable time frame? | Companies can:<br>1. Make data subject access request tools prominent<br>2. Make them age appropriate and easy to use<br>3. Make tools specific to the rights they support<br>4. Include mechanisms for tracking progress and communicating with you | » Lack of transparency regarding personal information usage<br>» Longevity of teen data that is meant to be point-in-time, which creates confidentiality and retention issues |
| *Appropriate data security procedures & fulfilling the business' duty of care* | For purposes of protecting the confidentiality, integrity, and accessibility of personal data, does the entity establish, implement, and maintain reasonable administrative, technical, and physical data security practices appropriate to the volume and nature of the personal data at issue? | » Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as appropriate.<br>» Consider existing ISO standards (e.g., ISO 27001) for data security.<br>» Follow appropriate encryption standards.<br>» Determine alignment with cyber security standards, as noted in federal and state cyber security laws. | » Data breach<br>» Inappropriate collection<br>» Violating duty of loyalty and duty of care |
| *Impact Assessments* | Do you conduct an impact assessment to assess the risks to teen or minor users? | » Before deploying a product designed for teenage users, complete a Data Protection Impact Assessment for such product's services and features.* | » Data breach<br>» Inappropriate collection, sharing without careful analysis of tradeoffs |

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Impact Assessments* | Would your organization feel comfortable sharing a copy or summary of DPIAs with us, to analyze the risk-reward equation? | » *Note: AADC preliminary injunction places the required nature of this into question, but it is a best practice. | » Violating duty of loyalty and duty of care |
| *User-generated content* | Are there mechanisms for users to flag and report harmful or illegal content/conduct? | » Make user-friendly flags available at the time they are needed.<br>» Provide technical controls to empower users to limit future potential for harmful engagement. | » Cyberbullying<br>» Image abuse<br>» Unsafe/unwanted contact |
| | Are users empowered to control their own experience and limit interaction with harmful users/content? | » Provide functionality to block, mute, or pause other users.<br>» Provide ability to filter keywords or reduce frequency of certain content.<br>» Provide ability to limit visibility of their own content, fine-tuned audience controls. | » Cyberbullying<br>» Unsafe/unwanted contact<br>» Digital reputation self-harm |
| | Are there business procedures in place to review and remove flagged content? | » Create and adhere to internal processes to review, escalate, and take action.<br>» Place ownership of this process with a team that has the resources to respond to volume.<br>» Work with verified mental health organizations to ensure that helpful mental health resources are not downranked or filtered in the same manner as harmful content. | » Cyberbullying<br>» Unsafe/unwanted contact<br>» Loss of trust in system/brand |
| | Are there business procedures in place to suspend or remove users who engage in harmful conduct? | » Implement technical features to monitor for inappropriate connections ("predator detection").<br>» Create and adhere to internal policies for suspending and removing based on strikes or extreme policy violations.<br>» Implement mechanisms to prevent banned users from opening new accounts. | » Cyberbullying<br>» Unsafe/unwanted contact |

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *User-generated content* | Are mechanisms for enhancing safety clearly communicated, at a level understandable by teens? | » Provide up-front disclosures.<br>» Explain the why of policies and mechanisms.<br>» Empower user buy-in and action (not top-down control). | » Learned helplessness |
| | Are the mechanisms conspicuous to teen users? | » Do not bury safety mechanisms in settings menus; instead, make them easy to find. | » Inadequate information for teen comprehension |
| | Do the mechanisms allow teens to exercise them anonymously? | » Provide the option to use safety mechanisms anonymously. | » Retribution from other users<br>» Ostracization or reputational harm within peer groups |
| | Are the mechanisms easy to use? | » Empower user buy-in and action (not top-down control). | » Inadequate information for teen comprehension |
| | Do you have a business policy and procedure for reporting illegal content to law enforcement? | » Consider mechanisms to report certain content types to relevant law enforcement (CSAM, reputable threats, violence, and self-harm).<br>» To avoid false positives, use manual reviews before reporting. | » Unsafe/unwanted conduct<br>» Brand/reputation harm<br>» Potential legal exposure |
| | Are any users able to react and respond to teen users' posts/UGC, such as on a social platform? | » Allow teen users to flag and remove unwanted reactions to their own user-generated content, including photo tags from other users. | » Cyberbullying<br>» Unsafe/unwanted contact |
| | Can a teen user restrict which types of users they can communicate with via direct messages? | » Give teen users control over which users can contact them directly in areas where direct messaging is possible. | » Unsafe/unwanted contact |
| | Are there business processes for monitoring unwanted/inappropriate behaviors, such as reactions or uses of posts/UGC? | » Automate flagging or monitoring with a manual review or escalation.<br>» Consider using community policy enforcement (users as moderators).<br>» Where feasible, establish a training program at your organization for community moderators to better align community moderation practices with safeguards for teen users. | » Harmful conduct may evade detection and enforcement of the Terms of Use |

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Content that could be considered inappropriate for teen audiences* | Is the content inappropriate for teen audiences? | » For U.S. audiences, consider third-party guides for appropriate content across specific age bands: e.g., ages 13-14, ages 15-17.<br>» Do not target salacious, incendiary, or highly polarizing content to teens (such as political topics).<br>» Avoid content that could be especially sensitive to teens or amplify existing insecurities (e.g., body odor, hair loss, weight). | » Exposure to age-inappropriate or potentially harmful or addictive content |
| *Content that could be considered inappropriate for teen audiences* | If aware of teenage users, are there mechanisms to flag and limit exposure to inappropriate content? | » Implement algorithmic content monitoring (e.g., adult content, hate speech, drug use).<br>» Automate suppression of identified harmful content.<br>» Flag, warn, and remove users for posting illegal content. | » Exposure to age-inappropriate or potentially harmful or addictive content |
| | If unaware of teenage users, are there disclosures to help users avoid inappropriate content by default? | » Consider implementing NSFW filters and 18+ content filters. | » Exposure to age-inappropriate or potentially harmful or addictive content |
| *The use of algorithms to curate content* | Can teen users tailor their content preferences? | » Empower users to adjust their preferences over time, giving them more transparency about what their aggregate viewing appears to be (see more of X, see less of Y).<br>» Give teenage users the ability to affect algorithmic content delivery by providing appropriate tools to down-rank unwanted content from future content delivery. | » Addictive behavior<br>» Self-harm<br>» Echo chamber/filter bubble effect |
| | Is it clear to teen users that engaging with content will result in receiving more of the same type of content? | » Provide information to teen users to explain why they are seeing specific content, for example due to the content they "Like" or the types of content they engage with for longer periods of time. | » Addictive behavior<br>» Echo chamber/filter bubble effect |
| | Is potentially harmful and/or addictive content amplified more than other types of content? | » Flag certain content that may be considered sensitive to teen users. | » Addictive behavior<br>» Self-harm |

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *The use of algorithms to curate content* | Are there business practices for monitoring and removing harmful/addictive content? | » Automate flagging or monitoring (particularly of hashtags, content review) with manual review or escalation.<br>» Continually monitor new "trends" emerging on spaces popular with teens that encourage harmful/addictive behaviors.<br>» Monitor for new detection avoidance behaviors, such as intentional misspelling (replacing letters with numbers) or other "code" words. | » Exposure to age-inappropriate or potentially harmful or addictive content |
| *Retention of personal information* | Do you change the way you use information about teens after they become adults? | » Minimize the potential of profiling adults based on teenage interests, behaviors, and activities. | » Teen information as part of a "permanent record" that follows into adulthood<br>» Increased risks of data breach |
| | Do you provide easy-to-use mechanisms for teens to delete or remove data in a granular manner? | » Give teens control over their digital footprint and allow for changes in behavior and interests to be reflected. | » Permanent record/digital footprint could impact/harm reputation<br>» Entrenching behavior |
| | Do you retain sensitive information collected from teens after they become adults? | » Review whether holding teen information for an extended period of time would potentially result in a bias or harm (whether or not that data is still being used). | » Potential for bias when relying on inaccurate or outdated information<br>» Overcollection |
| | How long do you retain information collected from known teens? | » Consider shortening retention periods of teen information when there is a reasonably known increased risk of harm. | » Teen data as part of a "permanent record" that follows into adulthood<br>» Increased risks of data breach<br>» Permanent record/digital reputation<br>» Entrenching behavior |

# Sharing of Teen Data

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Sharing of personal information with service providers and third parties* | Do you carefully consider the entities with which you share known teen data? | » Vet privacy practices relating to teen data of all service providers and data processors | » Increased risks of data breach, misuse of teens' information |
| | Do you have a governance document in place with service providers (and, where possible, all known third parties) with whom data is shared? | | |
| *Sharing of personal information with service providers and third parties* | Do you disclose the categories or names of the entities with which data is shared, and the purpose for which they are using teen information? | » Empower teen users to easily seek and request more information about which entities receive their information. | » Increased risks of data breach, misuse of teens' information |
| | Do you use or allow other entities to use teen information for purposes incompatible with their digital mental, or physical well-being or safety? | » Map data types to purposes and shared entities to help users and stakeholders understand potential risks and avoid harms. | » Increased risks of data breach, misuse of teen's information |

# Social Features

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Social interactions between users through direct messaging, commenting, friending, or any other means of contact* | Do you provide sufficient methods that would allow a teen user to report when content, conduct, or contact that puts teenage users at risk of harm? | » Provide teenage users a method to report content, conduct, or contact of other users that the teen user believes is harassing, bullying, soliciting, threatening, exploitative, violent, or otherwise harmful to a teen user's wellbeing.<br>» Methods of reporting should be available in all places on a platform where a teen user can interact with other users.<br>» Make reporting features clearly accessible to teen users, distinguished by a uniform design element on the site, and available whenever the teen user can see another user's post, comment, connection or friend request, direct message, forum post, chat, or other communication features.<br>» After a teen user submits a report, prevent the subject of the report from being able to contact the teen user by default, and clearly communicate this to the teen user.<br>» After a full review of the reported conduct or contact has been completed, follow up with the teen user who sent a report and communicate the finding and decision in the matter. | » Unsafe/unwanted contact |

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Making a user discoverable to other users through search features, friend recommendations, or other means* | Do you provide sufficient tools that empower the teenage user to prevent unwanted or harmful contact? | » Limit the ability of users to discover teen users or teen users' information until the teen user has approved discoverability for the other user.<br>» Approving discoverability for specific users could be performed by a method such as allowing teen users to select other users from existing device contacts, sharing an in-app QR code, or other technically feasible methods that put the teen user in control of their discoverability for other users. | » Unsafe/unwanted contact |
| *Allowing users to send messages to each other* | Do you provide sufficient safeguards that prevent teenage users from seeing inappropriate or unwanted messages from other users? | » Do not allow users to send unsolicited messages to a teen user unless the teen user has made themselves discoverable to the specific other user. | » Unsafe/unwanted contact |
| *Determining how to respond to reports of inappropriate or harmful content, conduct, or contact* | How can your organization adopt clear policies that communicate proper community standards and the potential sanctions that result from reported violations? | » Adopt a clear and easy-to-access code of conduct for users that specifies when content, conduct, or contact directed at a teen user would violate community standards and that explains the resulting punishment for users that violate these community standards.<br>» Adopt a tiered system of punishments and sanctions for violations of the code of conduct. This tiered system could include account strikes, feature limitations, permanent account bans, or any other restrictions that incentivize users to follow proper community standards, particularly when teen users may be the target of unwelcome or harmful conduct. | » Unsafe/unwanted contact |

# In-App Purchases

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Allowing teen users to perform in-app purchases* | Do you provide clear, prominent, and meaningful notice to parents/guardians that your product(s) allow in-app purchases? | » Display a notice on an application store page indicating the presence of in-app purchases, and when feasible, provide information in the store page description about how and when the application seeks account holder authorization for in-app purchases. | » Unwanted, unauthorized, and deceptive purchases |
| *Allowing a teen user to perform an in-app purchase using a parent or guardian's payment information* | Do you provide sufficient safeguards to prevent teen users from making unauthorized purchases with a parent/guardian's payment card? | » Require some form of technically feasible authorization from the adult payer (e.g., CVV input, one-time pin, password, push notification, etc.) before processing the payment.<br>To achieve this the app could either:<br>1. Seek authorization through these methods every time a teen user initializes a purchase with a parent/guardian's card; or<br>2. Provide a dashboard to the parent/guardian so that they can pre-approve and pre-disapprove of specific categories of in-app purchases. | » Unwanted, unauthorized, and deceptive purchases |
| *Resolving disputed in-app purchases involving charges made on teen user accounts* | Do you take sufficient steps to ensure that the process of resolving charges on a teen user's account does not involve unfair business practices? | » Provide an easy-to-access and expedited system for processing complaints of unauthorized and unwanted charges.<br>» Make unsubscribing to a recuring charge as easy as, or substantially similar to, the process to subscribe. | » Unwanted, unauthorized, and deceptive purchases |

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Resolving disputed in-app purchases involving charges made on teen user accounts* | | » Avoid the practice of suspending or deleting teen user's accounts for merely disputing in-app purchases with the platform or a financial institution. However, platforms may seek to restrict access to a teen user's account where a risk of legitimate security or fraud prevention concerns arise | |
| *Allowing a user to make in-app purchases through use of an instant purchase button* | Do you take steps to ensure that your application design does not lead to unwanted or unfair charges on a teen user's account? | » Avoid allowing teen users to make instant purchases or require the user to confirm their purchase so that the account is not charged erroneously upon a single click.<br>» Ensure that any purchase button is presented as a distinct design element—separated from other design elements by substantial non-interactive space on the display—so that users of any ability can avoid mistaking a purchase button for some other design element or pushing the button by accident. | » Unwanted, unauthorized, and deceptive purchases |

# Parental Tools

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Allowing a teen user's parent/guardian to monitor the child's online activity or track the child's location in real time* | Do you provide sufficient notice to a teen user that such monitoring can and does occur? | » Provide an obvious, in-application signal to indicate when a parent/guardian is monitoring or tracking the teen user. | » Limiting teen privacy or autonomy |
| *Allowing a parent or guardian to access teen user account information (posts, use metrics, information on direct messaging, etc.)* | What information is useful to parents/ guardians as a conversation starter about proper and safe use of technology? | » Seek a balance between providing information that can assist parental oversite while avoiding disclosing information that could violate a teen user's autonomy.<br>» Consider applicable law to guide what account information must be disclosed to parents/guardians in a given jurisdiction. | » Limiting teen privacy or autonomy |
| *Allowing a parent or guardian to alter a teen user's account or privacy settings* | How will teen users be made aware of these alterations? | » Provide a notification to the teen user that clearly explains how the setting has been altered and how the changed setting affects different functionalities of the product. | » Limiting teen privacy or autonomy |

# Research Practices

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Conducting market research that involves teen users* | Are there best practices with regard to privacy preserving techniques used on the data that you can adopt when conducting market research? | » Use methods of privacy preservation encryption/ anonymization/other techniques to prevent associating individual responses with teen participants.<br>» Provide the teen user and their parent/guardian with a clear, conspicuous, and easy-to-understand explanation of the scope and purpose of the research before the point of collection. | » Lack of transparency in the marketplace on teen perceptions toward their data usage |
| *Conducting trust and safety research for an online platform* | Are there meaningful partnerships your organization can form with outside organizations or researchers to better understand emerging harms on your online platform? | » Provide access to de-identified datasets (though use of an Application Programming Interface (API), access to a database, or other technically feasible and secure method) to trust and safety researchers employed at institutions of higher education and/or non-profit organizations so that researchers can assist identifying risks to teen users.<br>» Establish a cross-disciplinary Online Trust and Safety Oversite Committee (or equivalent body) at your organization to serve as your organization's primary governance body to research platform trust and safety.<br>Focus trust and safety research on teen users and the following potential harms:<br>» Mental health disorders or associated behaviors, including the promotion or exacerbation of self-harm, suicide, eating disorders, and substance use disorders;<br>» Patterns of use that indicate or encourage addiction-like behaviors; | » Lack of strong marketplace data about the effects, both positive and negative, regarding digital product and service usage. |

| When designing business practices that involve... | ...ask yourself... | ...and consider these practices... | ...to avoid these risks/harms. |
|---|---|---|---|
| *Conducting trust and safety research for an online platform* | | » Physical violence, online bullying, and harassment;<br>» Sexual exploitation, including enticement, sex trafficking, and sexual abuse of minors and trafficking of online child sexual abuse material;<br>» Promotion and marketing of narcotic drugs, tobacco products, gambling, or alcohol to minors; and<br>» Predatory, unfair, or deceptive marketing practices, or other financial harms. | |

# Appendix

## Background Research on Teen-Specific Privacy Harms


+ Danah Boyd, "It's Complicated: The Social Lives of Networked Teens," Yale University Press (2015), Link
+ Pamela Wisniewski, collected academic works on Adolescent Online Safety and Networked Privacy.
+ Global Teen Privacy Rules chart (BBB National Programs – TAPP convening).
+ "Privacy Matters: Parents and Teens Share Attitudes and Opinions," Common Sense Media, SurveyMonkey (2018), https://www.commonsensemedia.org/sites/default/files/uploads/pdfs/commonsense-surveymonkey.pdf.
+ "Unpacking Age Assurance: Technologies and Tradeoffs," Future of Privacy Forum (2023). https://fpf.org/blog/new-fpf-infographic-analyzes-age-assurance-technology-privacy-tradeoffs/.
+ "Trust & Safety Glossary of Terms," Digital Trust & Safety Partnership (2023). https://dtspartnership.org/glossary/.
+ "Guidelines for Industry on Child Online Protection," UNICEF (2015). https://sites.unicef.org/csr/files/COP_Guidelines_English.pdf
+ "A Comprehensive Resource for Tracking U.S. State Children's Data Privacy Legislation," Husch Blackwell (2023). https://www.huschblackwell.com/2023-state-childrens-privacy-law-tracker.
+ "Design Principles," Designing for Children's Rights (2022). https://childrensdesignguide.org/wp-content/uploads/2022/07/D4CR-Design-Principles-2.0-2022-07-12.pdf.
+ Gabrielle Shea & Sabine Neschke, "Tech policy Trifecta: Age Assurance Risks and Rewords," Bipartisan Policy Center (2023). https://bipartisanpolicy.org/blog/tech-policy-trifecta-age-assurance-risks-and-rewards/.
+ Key Takeaways: TikTok Testifies at House Energy & Commerce Committee Hearing (Mar. 2023) by Divya Sridhar, Ph.D.A
+ Not-So-Sweet Sixteen? Teen Online Privacy and Safety Faces New Policy Dilemmas (Aug. 2023) by BBB National Programs Privacy Initiatives Team
+ Injunction Junction: NetChoice v. Bonta and Securing the Future of Teen Online Privacy and Safety (Oct. 2023) by BBB National Programs Privacy Initiatives