# Senate Judiciary Committee
# Questions for the Record for Mr. Evan Spiegel
# CEO and Co-Founder of Snap, Inc
# Submitted February 28, 2024

**Sen. Dick Durbin (D-IL)**

**1.** For each year from 2019 to 2023, please provide the following:

**a**. the total number of users on your platform;

Approximate Global Average Annual Daily Active Users (DAU) is shown below.

| | Approximate Global Avg. Annual DAU |
|---|---|
| 2019 | 205M |
| 2020 | 245M |
| 2021 | 300M |
| 2022 | 354M |
| 2023 | 400M |

**b.** the total number of users under the age of 18 on your platform;

| | Approximate Global Avg. Annual DAU Aged 13-17 |
|---|---|
| 2019 | 34M |
| 2020 | 41M |
| 2021 | 50M |
| 2022 | 58M |
| 2023 | 60M |

**c.** the estimated number of users under the age of 13 on your platform;

Snapchat is not intended for use by people under the age of 13. When we learn an account user may be under 13 years old, we investigate and remove the account if warranted. We therefore do not track the number of Snapchatters who may be under age 13.

**d**. the number of users of your platform under the age of 18 who opted-in to your Family Center tool and were linked with a parent or guardian's account?

Approximately 200,000 parents use Family Center and about 400,000 teens have linked their account to their parents using Family Center.

**e.** your company's annual revenue;

2019 – approximately $1,716 million
2020 – approximately $2,507 million
2021 – approximately $4,117 million
2022 – approximately $4,602 million
2023 – approximately $4,606 million

**f.** your company's annual budget for trust and safety;

2019 - approximately $39 million
2020 - approximately $54 million
2021 - approximately $131 million
2022 - approximately $164 million
2023 - approximately $135 million

**g.** your company's annual budget to address online child sexual exploitation;

See above totals in (f), as this area of focus is incorporated in our trust and safety budget.

**h.** the total number of employees working to address trust and safety;

| Year | Total No. Performing Safety and Moderation Work (As of 12/31/23) |
|---|---|
| **2019** | 763: 79 (FTE), 684 (CW) |
| **2020** | 1,218: 99 (FTE), 1,119 (CW) |
| **2021** | 3,051: 148 (FTE), 2,903 (CW) |
| **2022** | 2,593: 124 (FTE), 2,469 (CW) |

| | |
|---|---|
| **2023** | 2,226: 163 (FTE), 2,063 (CW) |

**i.** the total number of employees working to address online child sexual exploitation.

Same answer as (h) above.

**2**. How did your company determine that 13 was the appropriate age for a child to begin using your platform?

In compliance with the Children's Online Privacy Protection Act (COPPA), Snapchat is not a service directed to children under the age of 13. When registering a Snapchat account, users are required to accept Snap's Terms of Service, acknowledge the Privacy Policy, and provide their date of birth. Users need to be at least 13 to create a Snapchat account, and the registration process is blocked if a user is under the age of 13. If we become aware that a Snapchat user is under the age of 13, we will terminate that user's account and delete the user's data. We also implement a safeguard that prevents 13-17 year old Snapchat users with existing accounts from updating their birthday to an age of 18 or above.

**3.** What legal obligation does your company have in the United States to ensure that your platforms are safe for children before they are launched?

As described in response to question 2, COPPA provides a legal framework for children's access to internet services. Snapchat is not a service directed to children under age 13. Users need to be at least 13 to create a Snapchat account, and the registration process is blocked if a user enters an age under 13. If we become aware that a Snapchat user is under the age of 13, we will terminate that user's account and delete the user's data. In 2014, Snap entered into an agreement with the FTC to establish and maintain a robust privacy program, which, among other things, involves pre-launch reviews of Snap's features and functionality. The mechanisms in place as part of these processes play a critical role in promoting safety when designing Snapchat features for all users, including our teenagers. Over the years, we have expanded the FTC privacy-by-design framework to also incorporate safety-by-design, and have created a holistic framework for privacy-and-safety by design, that considers a wide range of laws and regulations.

**4.** For users under the age of 18,

**a**. what are the default privacy settings for their accounts?

Snapchat was designed with privacy and safety in mind for all users, and we apply a high privacy bar for all users, including teens. For example, friend lists are private by default, and we don't offer settings to change that. Contact settings are limited to friends and phone contacts only – and can't be expanded. Location sharing is off by default, users under 18 are unable to create a Public Profile on Snapchat, and we don't allow under 18s to change their age to an age over 18.

**b**. what limitations are placed by default on content these users can access, content that will be directed toward them, and individuals they can communicate with?

We want Snapchat to be safe for everyone, and we offer extra protections for minors to help prevent unwanted contact and provide an age-appropriate experience. We have default content settings for teens that limit their exposure to shocking, suggestive, or other sensitive content on our broadcast surfaces. We also use age-gating to ensure that any advertising content is age-appropriate.

As a foundational safeguard, we've designed our service to require direct communication between friends to be opt-in, meaning people have to proactively choose who they communicate with. Friend lists are private on Snapchat, which not only reduces social pressure but also limits the ability of predators to find a person's friends on Snapchat. Snapchat's default "Contact Me" settings are set to friends and phone contacts only for all accounts, and can't be expanded. If a minor receives a friend request from someone they don't share a mutual friend with, we provide a warning before they start communicating to make sure it is someone they know. As a result, approximately 90% of friend requests received by minors on Snapchat are from someone with at least one mutual friend in common. Our goal is to make it as difficult as possible for people to be contacted by someone they don't already know.

**c**. can they change their default settings without the awareness of their parent or guardian, or without the consent of their parent or guardian?

Yes, users under 18 can change their default settings without the consent of their parent or guardian. However as part of our ongoing enhancement and evolution of our Family Center tool for teens and parents, we plan to introduce a new feature to give parents visibility into their teen's privacy settings.

**d**. in 2023, how many changed their default settings?

We do not possess this data.

**5.** If the default settings are different for users aged 16 and 17 than they are for users under the age of 16, please explain why your company takes this position, how this position was developed, and whether any company personnel voiced objections to or raised concerns about this position.

Default settings are the same for all users under 18.

**6**. What studies, research, summaries, or data does your company have reflecting the efficacy of its parental controls and child safety measures? Please provide these studies, research, summaries, or data.

In developing Snap's parental resource tool, Family Center, we took a comprehensive approach to find the right balance of features that gave parents insight to who their teens were interacting with on Snapchat, while still respecting the privacy and autonomy of teens. Our research highlighted how important it was to provide useful tools for parents that improve visibility into their teen's activity on our service and expand education on safety best practices, to safeguard teen privacy and limit overly invasive tools, and to be mindful of different family dynamics across cultures and marginalized groups. This research included:

- Direct user feedback, submitted by our users though our support site
- Focus groups that interviewed parents and teens separately and together to get their feedback on which tools would be most useful
- User research studies that surveyed parents and teens on their perception of safety on Snapchat, and gauged their awareness of Family Center and parental tools on other services
- Benchmark studies that survey parents' sentiment towards Snapchat and parental tools and how this changes over time
- Feedback sessions with dozens of online safety experts, including academics, researchers, safety experts, members of parent groups, and NGO leaders to inform our design of Family Center features
- Deep dive discussions with our Safety Advisory Board on their recommendations for our parental tools

**7**. Concerning international law,

> **a**. what steps have your company and its subsidiaries taken to comply with the European Union's Digital Services Act?

At Snap, privacy, safety, and transparency have always been core to how we operate. We have protections in place for all members of our community and offer additional safeguards for our teenage Snapchatters. Our long-standing values are aligned with the principles of the European Union's Digital Services Act (DSA) and we share their goals to create a safe online environment. We made a number of changes to our service, including (1) giving Snapchatters the ability to control the content they're shown, (2) a new notification and appeals process for content or account removals, (3) updates to our advertising practices, and (4) appointing compliance officers.

> **b**. what steps has your company and its subsidiaries taken to comply with the United Kingdom's Online Safety Act?

The United Kingdom's Online Safety Act (OSA) is not yet in effect. However, our long-standing privacy and safety practices, and work relating to other compliance efforts, provides a strong foundation for new requirements that will come into effect under the OSA in the coming years. We are incorporating OSA requirements in our risk assessments and privacy-and-safety by design review process.

> **c**. what steps has your company and its subsidiaries taken to comply with Australia's Online Safety Act?

Snap's longstanding robust privacy and safety practices provided a strong foundation for compliance with Australia's Online Safety Act, and we did not need to make significant changes to our best practices to comply. The requirements of Australia's Online Safety Act are incorporated as part of our ongoing privacy-and-safety by design review process.

> **d**. if those laws create a safer, healthier online experience for kids on your platforms, do you commit to implement these changes in the United States? If not, why not?

Snap has in place protections for all members of our community and offers additional safeguards for our teenage Snapchatters, including our users in the United States, and all users benefit from safety enhancements we've made as part of compliance with the laws mentioned above. Our long standing values are aligned with the principles of the European Union's Digital Services Act (DSA) and other safety and transparency laws, and we share their goals to create a safe online environment. We also support the Kids Online Safety Act, introduced in the Senate. We have already implemented many of its provisions such as mandating appropriate default privacy settings, providing safeguards for teens (including additional privacy settings that protect their privacy and offer them control over their experience), offering parental tools, and limiting the collection and storage of personal information.

**8**. In 2022, Snapchat was used by 90% of U.S. residents aged 13-24, making Snapchat a prime platform for predatory users to target children. According to Snap's Terms of Service convicted sex offenders are not permitted to use its services. Despite this policy, registered sex offenders have been found to regularly make accounts and further victimize and exploit children using Snapchat.

For example, in August 2023, a registered sex offender with prior convictions in Illinois and Michigan was sentenced to 25 years in prison for luring a 15-year-old girl over Snapchat and engaging in sexual activity with her. Similarly, in July 2023, a registered sex offender was arrested in Texas and charged with child trafficking to engage in sexual conduct. The offender used Snapchat to meet his potential victims online. What steps does Snap take to enforce its policy against registered sex offenders and ensure sex offenders are actually kept off of your platform?

These crimes are vile and abhorrent. We do not tolerate such accounts on Snapchat and we have in place policies allowing us to take swift action and help bring predators to justice. If we learn an account is alleged to be used by a registered sex offender, our teams immediately investigate and take action as appropriate. We receive tips from law enforcement, news media, and other partners, and we act on these referrals. Upon confirming that an account is used by a registered sex offender, the account is immediately disabled and the device is blocked.

**9**. Snap uses photo recognition technologies to detect CSAM on its platform, but this technology can only detect known CSAM. As a result, newly-created CSAM often goes undetected on Snapchat. As a platform where users are overwhelmingly sharing new pictures and videos, how is Snap working to prevent the use of its platform for the creation and trafficking of CSAM?

We ban sharing nude images of anyone under 18 and want to protect our community from the devastating consequences that can come if this content falls into the wrong hands. If we find this content, we report it to NCMEC. In 2023, for example, more than 225,000 of the approximately 690,000 NCMEC reports Snap submitted originated from users reporting content to us. We empower users to report this content with easy-to-use in-app reporting tools, and we are exploring additional technical solutions for detecting this content.

**Sen. Lindsey Graham (R-SC)**

**1**. Do you support S. 1207, the bipartisan EARN IT Act? Why or why not?

We support the Senate Judiciary Committee's efforts to better protect young people online, and are supportive of the Earn It Act's underlying goals. As currently drafted, we have some concerns with this bill. The broad liability provisions in the Earn It Act could be used to sweep up services, like ours, in a wave of civil litigation that distracts from our core safety mission, despite our adherence to best practices. A FOSTA-SESTA approach would allow for liability against services that are truly bad actors—those who are affirmatively trying to help criminal bad actors on their service, or willfully turning a blind eye to known instances of illegality—while still protecting services that are working tirelessly to do their best to stop bad actors.

**2**. What measures are you taking to prevent and address sextortion, including financial sextortion, on your companies' platforms?

This conduct is illegal and abhorrent, and we take active steps to identify and prevent such exploitation as well as empowering users to identify and report suspicious contact.

We combat this criminal activity by:

- Making it difficult for strangers to search for, find, or contact teens.
- Warning teens if they receive a friend request from another person who isn't a mutual friend or phone contact.
- Keeping friend lists private and preventing teens from having public profiles — which helps prevent criminals from using Snapchat to target a teen's friends
- We proactively detect accounts attempting to engage in sextortion and disable them. When we remove sextortion-related content, we also retain it for an extended period of time in case law enforcement wants to follow up with a valid legal request.
- We've added an in-app reporting option specifically for sextortion ("They leaked/are threatening to leak my nudes.") to make it easier for our community to report such abuse to us. When we receive such a report, we take action quickly – usually within 30 minutes.
- We also educate teens about the dangers of this type of crime and urge them to use our in-app reporting tools.

This is very important because young people may feel afraid to report the problem to their parents or caregivers.

**a**. What methods are in place to detect and disrupt this type of abuse in real time?

Please see response to question 2.

**3**. Please provide the committee statistics on how long it takes your company to respond to various types of legal process from law enforcement?

Currently, we respond to most legal process within two to three weeks. We respond to most requests for voluntary disclosure of data in instances involving imminent threat to life or serious physical injury within thirty minutes.

**4**. Do you notify your users when law enforcement serves subpoenas/summons for subscriber information and specifically requests not to notify the subscriber/user?

We do not notify users when law enforcement provides a nondisclosure order or when we believe an exceptional circumstance exists, such as cases involving child exploitation, or the threat of imminent death or serious bodily injury, such as the sale of fentanyl. When law enforcement does not provide a nondisclosure order, we will follow up to see if they plan to obtain a nondisclosure order before we take steps to notify the user.

> **a**. If you notify the subscriber, how long do you wait until notification goes out?

Snap will not notify a user until we have confirmation from law enforcement that they understand the user will be notified, that law enforcement does not intend to seek a non-disclosure order and we have given law enforcement the opportunity to let us know whether the case does not fall within one of the exempted categories listed in the answer above.

> **b**. Are you aware that by notifying the subscriber about a law enforcement subpoena for their subscriber information that you are jeopardizing critical evidence that could be erased before law enforcement can serve warrants?

The existing legal framework (the Stored Communications Act) permits law enforcement to submit a preservation request, and Snap does not notify users upon receipt of a preservation request. Snap complies with such requests to preserve account data for up to 180 days as authorized by law. A preservation is a snapshot in time of a user's available data, including available basic subscriber information, metadata, geolocation data, and content (*e.g.*, Chats, Stories, and Memories) and is held in an offline file where it cannot be accessed by the user.

We do not provide user notice when providing notice is prohibited by a court order or by other legal authority; or when we believe an exceptional circumstance exists, such as cases involving child exploitation, or the threat of imminent death or serious bodily injury, such as the sale of fentanyl. When law enforcement believes that critical evidence would be erased as a result of user notification, they commonly seek and are granted a non-disclosure order. Due to the use of non-disclosure orders and Snap's policy to exempt cases involving the exceptional circumstances noted above, fewer than 5% of account holders for whose accounts data was sought were notified of legal process between June and December 2023.

**c**. Would your company agree to a 90-day non-disclosure to subscribers to allow law enforcement ample time to secure proper legal process?

A nondisclosure period is already provided in existing law—the Stored Communications Act—upon submission of a valid court order by federal or state law enforcement. We do not provide user notice when providing notice is prohibited by a court order or by other legal authority. We also choose not to provide notice when law enforcement provides us with information indicating an exceptional circumstance exists, such as cases involving child exploitation, or the threat of imminent death or serious bodily injury, such as the sale of fentanyl.

**5**. Do you actively seek out and incorporate feedback and insight from survivors of online sexual exploitation to improve your trust and safety policies and practices and to prevent and disrupt child sexual abuse material (CSAM) production and distribution on your platform? Can you provide examples?

**a**. If not, please explain.

One of our Safety Principles at Snap is that we strive to be victim- and survivor-informed in all our efforts, including child sexual exploitation and abuse. We have the honor of representing the technology industry on the international Policy Board of the WeProtect Global Alliance, which includes representation of a disclosed survivor. These board members' contributions have impacted our thinking on a broad range of issues. We have also engaged with survivors directly and indirectly at CSEA-related conferences and events via our Safety Advisory Board, and we regularly engage with experts and nonprofits in this area.

**6**. During our hearing, you testified that you collaborate with parents and parent organizations to create mechanisms to keep children safe online. Please elaborate and cite examples of your company's work with non-employee parents and parent organizations.

We consulted with parents as part of a series of focus groups in developing our parental resource tool, Family Center, and with nearly 40 child safety experts to seek feedback and input before the launch of Family Center. We are also active Family Online Safety Institute members, support ConnectSafely.org, and collaborate with Protect Young Eyes. In addition, we work closely on national public awareness campaigns with Song For Charlie, a group started by Ed and Mary Ternan, who lost their son to fentanyl poisoning, and regularly consult members of our Safety Advisory Board, who engage with parents and caregivers globally.

**7**. Why does your company have the age limit of 13 years old for a user to sign up for an account?

In compliance with the Children's Online Privacy Protection Act (COPPA), Snapchat is not a service directed to children under age 13. When signing up for Snapchat, users are required to accept Snap's Terms of Service, acknowledge the Privacy Policy, and provide their date of birth.

Users need to be at least 13 to create a Snapchat account, and the registration process is blocked if a user is under the age of 13. If we become aware that a Snapchat user is under the age of 13, we will terminate that user's account and delete the user's data. We also implement a safeguard that prevents younger Snapchat users with existing accounts from updating their birthday to an age of 18 or above. Specifically, if a Snapchat user between the age of 13 to 17 attempts to update their year of birth to reach an age over 18, we will prevent the change.

**a**. Why not younger or older?

Please see response to question 7.

**8**. How many minors use your platform? How much money does your company make annually from these minors?

In 2023, there were approximately 60 million 13-17 year old daily active users on average globally. In 2023, Snap's global revenue from minors was approximately $437M.

**9**. What percentage of your employees work on trust and safety and how much money does your company invest annually in trust and safety?

Approximately 20% of our team, including both employees and contingent workers, works on safety – including our moderation teams, trust and safety teams, law enforcement teams and more. In 2023, we spent approximately $135 million on personnel costs for this team.

**10**. It is sometimes challenging for law enforcement conducting criminal investigations to determine the true identity of a person behind a name on social media or other online platforms, and whether an online identity is an actual person. What are you doing to validate the true identity of users – or the fact that a user is a human – when they create an account on your platforms?

We believe Snapchat can help people build stronger and healthier relationships with the most important people in their lives. To support that goal, we work everyday to help our community have a safe experience on our service – it's not only the right thing to do, it's essential to our mission. A key part of this work is collaborating with law enforcement, and we have a global Law Enforcement Operations team that works around the clock to support law enforcement investigations.

While messages on Snapchat delete by default – designed to reflect the nature of real-life conversations between friends – we can preserve available account information and content upon receipt of a valid law enforcement request.

To help build confidence that a new user is in fact a legitimate person, we prompt users during the account registration flow to verify their phone number or email address provided. We are also vigilant in regard to accounts being created through suspected automation (e.g. spam actors). We conduct risk analysis during account creation (and also post account creation) using continuously curated technical and behavioral signals to tell apart inorganic or undesired traffic coming on to our service.

**11**. Is your company using safety technology to detect and prevent live video child sexual abuse on your platforms and apps that allow users to stream or share live video? If not, please explain.

Snapchat does not have video capabilities that would permit users to live-stream or broadcast live video.

> **a**. Has your company tested that or similar technology? If not, are you developing similar technology to address child sexual abuse in live video?

See response to Question 11.

**12**. How are you measuring if your trust and safety policies, practices, and tools are effective in protecting children from sexual abuse and exploitation on your platform?

> **a**. What specific metrics or key performance indicators do you use?

Our semi-annual transparency reports are an important tool to hold ourselves accountable and share information and updates on our efforts to combat violating content and accounts on our service. You can find our latest Transparency Report here. Our main Transparency Report includes statistics relating to the Violative View Rate and our California transparency page links to our new California Terms of Service Report. This report, in turn, includes a range of safety-related metrics, including providing the Violative View Rate for individual categories of harms, as well as the Violative Viewer Rate which discloses how many viewers saw the content as a percentage of all active users over a period of time, both for the U.S. and globally.

**13**. Is your company using language analysis tools to detect grooming activities? If not, please explain.

No, we do not use language analysis tools to detect grooming. We believe there are other tools like network analysis that can detect and prevent grooming activities without compromising the privacy of user communications.

We are not aware of grooming-detection technology based on language analysis that has achieved the sufficiently high levels of precision required in light of the privacy considerations,

but we are actively exploring other metadata and content signals that can help uncover bad actor accounts.

**a**. What investments will your company make to develop new or improve existing tools?

We have already deployed features that limit the discoverability of minors via Search and Quick Add to people they have multiple friends and contacts in common with, which is a deterrent to grooming because it makes it difficult for strangers to request to connect with minors. We will continue to invest in more advanced strategies like this to make it even more difficult for strangers to find minors on the service. Additionally, we released an "in chat warning" to minors, surfacing block and report options at the top level, if they become friends with someone outside of their existing friend network. We will expand on this feature to incorporate more risk signals and provide even stronger warnings to minors in certain cases (e.g. if the other user has been reported before).

**14**. What resources have you developed for victims and survivors of abuse on your platforms?

As part of our overall effort to prioritize the mental health of Snapchatters, in 2020, we launched Here For You, a proactive in-app support system for Snapchatters who may be experiencing a mental health or emotional crisis by surfacing resources from expert organizations when Snapchatters search on a range of mental health-related topics, including eating disorders, anxiety, stress, depression, hate speech, bullying, suicidal thoughts, and more. When our Trust & Safety team recognizes a Snapchatter in distress, they will forward self-harm prevention and support resources, and notify emergency response personnel as appropriate. The resources that we share are available on our global list of safety resources, and these are publicly available to all Snapchatters.

**15**. What is your response to requests for content removal from CSAM survivors and other members of the public?

We take prompt action when we receive reports of CSAM, generally responding within 15 minutes. We also prioritize working with experts on programs like NCMEC's Take It Down and the Stop NCII database which gives us even greater access to hashes of illegal content that we can then leverage to proactively identify and remove offending content from Snapchat.

**16**. Some call Snapchat "dangerous by design," given the platform's disappearing photo feature, which makes it easy for predators to hide their crimes and giving naïve users a false sense of security. In which app functions do you scan for child sexual abuse material (CSAM)?

The sexual exploitation of any young person is horrific, illegal, and against our policies.

We prevent the distribution of CSAM in three key ways:

- We use cutting edge technology – PhotoDNA and CSAI Match – to proactively identify known CSAM photos and videos uploaded to Snapchat and report them to NCMEC.
- When we enforce against illegal and abusive content, we retain it for an extended period so that it is available if law enforcement want to follow up with a valid legal request.
- We take urgent action when we receive user reports of CSAM, generally responding within 15 minutes.

**17**. What safety messaging does Snap provide to its younger users around online safety, especially as it relates to online enticement and financial sextortion?

In 2023, we launched four new "Safety Snapshot" episodes in-app to help raise awareness and educate our community about various online sexual-related risks, namely: sexting and nudes, financial sextortion, child sex trafficking, and child online grooming for sexual purposes. Safety Snapshot is our official in-app channel for online safety and privacy advice and guidance. These episodes seek to speak to teens in a relatable language and style, and offer links to helpful resources. All four of the episodes were reviewed by experts at the National Center for Missing and Exploited Children (NCMEC) prior to release.

We have also provided users on Snapchat with safety messaging regarding the risks of fentanyl poisoning and counterfeit prescription drugs. We developed and made available an in-app education portal called "Heads Up" that distributes content from expert organizations such as Song for Charlie, Shatterproof, the CDC and the Substances and Mental Health Services Administration. If someone on Snapchat searches for drug-related keywords, Heads Up will show relevant educational content designed to dissuade engagement and ultimately prevent harm to our community.

Additionally, in partnership with Song for Charlie, we developed a video advertising campaign that has been viewed over 260 million times on Snapchat, and rolled out a new national filter that raises awareness of the dangers of fentanyl and counterfeit pills and directs Snapchatters to the Heads Up educational portal.

Finally, Good Luck America, a Snap Original news show, produced a special edition series of episodes devoted to educating our community about the fentanyl crisis.

**18**. How does Snap age assure and verify its users to ensure young children are not accessing its Platform?

In our Terms of Service, Privacy Policy and other documentation, we make clear that Snapchat is intended for users 13 years old or older. When registering a Snapchat account, users are required to accept Snap's Terms of Service, acknowledge the Privacy Policy, and provide their date of birth. Accordingly, the registration process is blocked if a user declares that they are under the age of 13. If we become aware that a Snapchat user is under the age of 13, we will terminate that

user's account and delete the user’s data. We also implement a safeguard that prevents younger Snapchat users with existing accounts from updating their birthday to an age of 18 or above. Specifically, if a Snapchat user between the age of 13 to 17 attempts to update their year of birth to reach an age over 18, we will prevent the change.

**Sen. Chuck Grassley (R-IW)**

**Directions**

*Please answer each question to the fullest possible extent. If your platform is unable to answer a particular question or does not have requested data, explain why. Each question refers to your company in addition to any corporate affiliates, including parent and subsidiary companies.*

**1.** Current law requires that a provider of a report of suspected CSAM to the National Center for Missing and Exploited Children's (NCMEC) CyberTipline preserve "any visual depictions, data, or other digital files that are reasonably accessible and may provide context or additional information about the reported material or person" for a minimum of 90 days. 18 U.S.C. 2258A(h)(1-2). The recent explosion of suspected abuse has presented unprecedented challenges for law enforcement to follow up on leads before companies discard or delete essential data and information. There is nothing preventing tech companies from preserving relevant material beyond the statutorily-mandated 90-day period.

> **a.** How long does Snap voluntarily preserve and retain data contained in and related to its reports to the CyberTipline?

Snap voluntarily preserves and retains all available data on accounts reported to the CyberTipline for approximately 180 days, twice the legally mandated period. In addition, when we enforce against illegal and abusive content, we retain it for an extended period so that it is available if law enforcement want to follow up with a valid legal request.

> **b.** The massive influx of reports to the CyberTipline naturally results in law enforcement entities having to conduct and finish investigations beyond 90 days of an initial report to the CyberTipline. Retaining relevant information for longer periods could significantly advance law enforcement's ability to thoroughly investigate leads. If Snap only preserves and retains this information for the minimum 90-day period, why does it do so when preserving this data longer could significantly enhance and prolong law enforcement's ability to investigate and prosecute child predators?

Snap already retains all available data on accounts reported to the CyberTipline for approximately 180 days.

> **c.** Please confirm if Snap stores and retains the following information relating to reports to the CyberTipline:
>
> > **i.** IP addresses

Yes, assuming this question is asking whether this category of data is preserved in connection with accounts reported to the CyberTipline.

**ii.** Screen Names

Yes, assuming this question is asking whether this category of data is preserved in connection with accounts reported to the CyberTipline.

**iii.** User Profiles

Yes, assuming this question is asking whether this category of data is preserved in connection with accounts reported to the CyberTipline.

**iv.** Associated Screen Names (by IP address and associated emails)

It is unclear what information the question seeks but Snap preserves a record of usernames and display names for accounts reported to the CyberTipline.

**v.** Email addresses

Yes, assuming this question is asking whether this category of data is preserved in connection with accounts reported to the CyberTipline.

**vi.** Geolocation data

Yes, assuming this question is asking whether this category of data is preserved in connection with accounts reported to the CyberTipline.

**d.** If Snap does not retain or store any of the above types of information in question (c), please explain why.

N/A

**e.** Please list any other information Snap retains and preserves for law enforcement purposes not listed above in question (c).

Snap preserves and retains available account information on accounts reported to the CyberTipline for 180 days. In addition to the data points listed above, this includes additional subscriber information, available communications content, and stored images and videos, among other data points.

**f.** Does Snap flag screennames and associated email addresses to suspected accounts that violate Snap's terms of service?

When Snap files a NCMEC report, the report includes the account's username and display name, as well as subscriber information, including email address, if applicable.

**2.** How does Snap prioritize urgent requests for information from law enforcement and what is Snap's response time to urgent requests?

Snap maintains a 24/7 emergency disclosure request form available to law enforcement globally for cases involving an imminent threat to life or serious physical injury. Snap responds to most such requests in under thirty minutes.

**3.** What is Snap's average response time to service of legal process from law enforcement for CSAM-related information?

Snap responds to most legal process, including legal process pertaining to CSAM-related information, within two to three weeks.

**4.** In 2023, the tech industry as a whole slashed more than 260,000 jobs. And in the first four weeks of this year, another 25,000 jobs were cut.

**a.** For each year, between 2018 and 2023, how many U.S. based employees did you have at Snap?

| Year | Total No. of US Employees |
|---|---|
| **2018** | FTE: 2,298 |
| **2019** | FTE: 2,378 |
| **2020** | FTE: 2,786 |
| **2021** | FTE: 3,965 |
| **2022** | FTE: 3,686 |
| **2023** | FTE: 3,731 |

**i.** Of these employees, how many were sponsored on H-1B visas?

| Year | Total No. of US Employees on H-1B Visas |
|---|---|
| **2018** | 323 |

| | |
|---|---|
| **2019** | 345 |
| **2020** | 410 |
| **2021** | 564 |
| **2022** | 446 |
| **2023** | 468 |

**ii.** For each year, between 2018 and 2023, how many H1-B visa applications did Snap submit?

| Year | Total No. of H-1B Visa Petitions Submitted (including amendments and extensions) |
|---|---|
| **2018** | 173 |
| **2019** | 254 |
| **2020** | 226 |
| **2021** | 359 |
| **2022** | 314 |
| **2023** | 248 |

**b.** For each year, between 2018 and 2023, how many employees based outside the U.S. did you have at Snap?

| Year | Total No. of Non-US Employees Globally (incl. China) | Total No. of Employees in China |
|---|---|---|
| **2018** | FTE: 586 | FTE: 49 |
| **2019** | FTE: 817 | FTE: 45 |
| **2020** | FTE: 1,077 | FTE: 47 |
| **2021** | FTE: 1,696 | FTE: 68 |
| **2022** | FTE: 1,602 | FTE: 60 |
| **2023** | FTE: 1,558 | FTE: 68 |

**i.** Of these employees, how many were based in China?

Please see response to question 4.b.

**c.** For each year, between 2018 and 2023, how many employees in total did Snap terminate, fire, or lay off?

| Year | Total Employee Involuntary Attrition Globally | Total Employee Involuntary Attrition - US |
|---|---|---|
| **2018** | FTE: 324 | FTE: 297 |
| **2019** | FTE: 72 | FTE: 67 |
| **2020** | FTE: 37 | FTE: 26 |
| **2021** | FTE: 53 | FTE: 40 |
| **2022** | FTE: 1,266 | FTE: 868 |
| **2023** | FTE: 337 | FTE: 162 |

**i.** Of these employees, how many were based in the United States?

Please see response to question 4.c.

**ii.** Did Snap fill these newly vacant positions with employees sponsored on H1-B visas? If so, how many?

We do not possess this information, however, we have provided the total number of employees sponsored on H1-B visas by the end of each year in response to question 4(a)(i), and total petitions filed in response to question 4(a)(ii).

**iii.** Were any duties and/or functions previously performed by laid-off employees transferred to or performed at any point by employees sponsored on H1-B visas? If so, which duties and/or functions?

Please see response to question 4.c.ii.

**d.** For each year, between 2018 and 2023, how many employees performing work related to child safety did Snap terminate, fire, or lay off?

| Year | Total Involuntary Attrition of Safety & Moderation Employees |
|---|---|
| **2018** | FTE: 14 |
| **2019** | FTE: 0 |
| **2020** | FTE: 1 |
| **2021** | FTE: 1 |
| **2022** | FTE: 26 |
| **2023** | FTE: 4 |

**i.** Of these employees, how many were based in the United States?

| Year | Total No. of U.S. Involuntary Attrition of Safety & Moderation Employees |
|---|---|
| **2018** | FTE: 11 |
| **2019** | FTE: 0 |
| **2020** | FTE: 1 |
| **2021** | FTE: 1 |
| **2022** | FTE: 17 |
| **2023** | FTE: 2 |

**ii.** Did Snap fill these newly vacant positions with employees sponsored on H1-B visas? If so, how many?

We do not possess this information, however, we have provided the total number of employees sponsored on H1-B visas by the end of each year in response to question 4(a)(i), and total petitions filed in response to question 4(a)(ii).

**iii.** Were any duties and/or functions (specifically relating to child safety) previously performed by laid-off employees transferred to or performed at any point by employees sponsored on H1-B visas? If so, which duties and/or functions?

Please see response to question 4.d.ii.

**iv.** How have layoffs impacted Snap's ability to protect children on its platforms?

Snap's reduction in force did not impact our ability to do safety-related work, nor our commitment to safety-related initiatives.

**v.** Does Snap have any plans to increase staff responsible for child safety operations or otherwise optimize its child safety operations?

We are constantly assessing our staffing needs to ensure that we are appropriately staffing these core and important initiatives.

**5.** On January 30, 2024, the Tech Transparency Project (TTP) published an article on their website called, "Meta Approves Harmful Teen Ads with Images from its Own AI Tool". In summary, TTP, using Meta's "Imagine with Meta AI" tool generated inappropriate images such as young people at a pill party or other vaping. These images with text were submitted to Facebook as advertisements targeting users between ages 13-17 in the United States. TTP reported that Facebook approved the advertisement, despite it violating its own policies, in less than five minutes to run on the following platforms:

Facebook, Instagram, Messenger, and Meta Quest. Meta. Over the course of a week, TTP submitted the advertisements with the same end result: Facebook approving them. TTP reported that they canceled these advertisements before their scheduled publication, but it illustrated the repeated failures of Facebook to properly moderate content. This is just one example of what other non-government organizations and others have uncovered across social media platforms.

**a.** How often a month do Snap employees conduct quality checks on Snap's policies and safeguards for child accounts?

Snap employees conduct quality checks regularly, including as part of daily audits of our enforcements (which also includes reviews of our policy) and weekly policy calls with our Policy team and 3rd party vendors who support Snap's content moderation efforts. A cross-functional group also meets on a regular basis to discuss safety efforts on Snap and child safeguards. We also conduct adversarial testing work to mimic ways bad actors may attempt to abuse our product and take those learnings to continue to improve our safeguards.

**b.** In which departments, components, or units of the company does Snap have staff dedicated to performing this type of work?

We believe that safety is a shared responsibility. We have teams in Product, Engineering, Operations, Policy, and Legal that support safety.

**c.** How many employees make up these departments, components, or units?

We have over 2,200 employees and contingent workers that support safety efforts at Snap. The majority of these personnel support trust and safety and content moderation.

**d.** If a violation is found, what action is taken, and how quickly is action taken?

Our dedicated Trust and Safety team works 24/7 to review reports and take appropriate action—in the vast majority of cases, we respond to reports and concerns within hours of receiving a report. Please refer to our Transparency Report that provides a breakdown of turn around times for actioning harmful content.

**6.** Social media companies claim they are investing in company components dedicated to safety, and that their platforms are safe for children. However, children continue to be exploited daily across these platforms.

**a.** What have Snap's revenue and profit figures been for the last three years (2021-2023)? Please provide figures broken out per year. Do not provide percentages.

Revenue:
2021 – $4,117 million
2022 – $4,602 million
2023 – $4,606 million

Profit/Loss:
2021 - $488 million net loss
2022 - $1,430 million net loss
2023 - $1,322 million net loss

**b.** How much has Snap spent in advertising for the last three years (2021-2023), broken out per year?

FY21: approximately $221 million
FY22: approximately $309 million
FY23: approximately $269 million

**c**. How much of Snap's resources spent on advertising has been devoted to advertising Snap's safety initiatives and efforts for the last three years (2021- 2023), broken out per year?

Much of our efforts to educate users about safety initiatives are through in-app notifications and education. When we offer new safety features, we utilize notifications to help Snapchatters understand the feature. We also have an in-house produced Snapchat channel dedicated to safety.

Safety Snapshot covers a range of safety topics such as sextortion, bullying, drugs, and other harmful behavior and educates Snapchatters on what they can do to protect themselves.

In 2022, with the launch of Family Center, Snapchat's parental settings tool, we dedicated $100,000 for media spend to fund advertising awareness for this initiative. This was largely to educate parents (who may be less familiar with our service) about a new tool to help them understand how their teens are using Snapchat.

**d**. To get an understanding of how your company has invested and plans to invest in its components dedicated to child safety functions, what are the annual budgets for Snap's child safety-related components for the last three years (2021-2023)?

2021 - approximately $131 million
2022 - approximately $164 million
2023 - approximately $135 million

**e**. What is the current anticipated (2024) budget for Snap's child safety-related components?

2024 Expected - approximately $142 million

**f.** Provide the number of staff employed in Snap's child safety-related components for the last three years (2021-2023).

| Year | Total No. Performing Safety & Moderation Work (As of 12/31/23) |
|---|---|
| **2021** | 3,051: 148 (FTE), 2,903 (CW) |
| **2022** | 2,593: 124 (FTE), 2,469 (CW) |
| **2023** | 2,226: 163 (FTE), 2,063 (CW) |

**g.** How much is that compared to Snap's other components for the same period? (Please provide a breakout per year. Do not provide percentages.)

| Year | Total No. of Snap FTEs and CWs (As of 12/31/23) | Total No. Performing Safety & Moderation Work (As of 12/31/23) |
|---|---|---|

| | | |
|---|---|---|
| **2021** | 11,129: 5,661 (FTE), 5,468 (CW) | 3,051: 148 (FTE), 2,903 (CW) |
| **2022** | 10,618: 5,288 (FTE), 5,330 (CW) | 2,593: 124 (FTE), 2,469 (CW) |
| **2023** | 10,620: 5,289 (FTE), 5,331 (CW) | 2,226: 163 (FTE), 2,063 (CW) |

**h.** How many staff are currently employed in Snap's child safety-related components?

We believe that safety is a shared responsibility. We have teams in Product, Engineering, Operations, Policy, and Legal that support safety. We have over 2,200 employees and contingent workers that support safety efforts at Snap. The majority of these personnel support trust and safety and content moderation.

**i.** What are the roles, responsibilities, and functions of Snap's child safety-related components?

Snap has many core teams across the company working on Child Safety, including those that work across safety of all our features. These teams include Product, Engineering, Operations, Policy, and Legal.

**j.** Are any other components responsible for the monitoring of CSAM on Snap's platform(s)?

As mentioned, Snap has many core teams across the company working on Child Safety, including those that work across safety of all our features. When our Trust & Safety team identifies CSAM content, they quickly remove the content and enforce against the appropriate account(s).

**k.** What, if any, third parties does Snap employ or contract with to address CSAM material on its platforms?

In addition to review by Snap employees, over the last three years, Snap has contracted several third parties to assist in review of CSAM material. These included Accenture, Telus, and Oddacious. Additionally, Snap contracts with an intelligence vendor that helps identify violative content on other services and across the internet (and dark web) implicating Snapchat accounts. We then promptly review those reports, investigate the accounts, and remove offending content.

**i.** What are the roles and responsibilities of these third parties?

Their responsibilities include an initial review of user safety reports as defined by our internal moderation processes and then, if needed, escalation to our full-time employees as instructed in our processes.

**ii.** What is the breakdown of cost per third party over the last three years (2021-2023)?

These costs are included in the overall Trust & Safety and Content Moderation Budget. Those include:

2021 - approximately $131 million (includes Vendor cost of ~$98 million)
2022 - approximately $164 million (includes Vendor cost of ~$112 million)
2023 - approximately $135 million (includes Vendor cost of ~$86 million)

**7.** Of all reports sent by Snap to the National Center for Missing and Exploited Children, how many reports were self-generated from victim users for the last three years (2021- 2023)? Please provide the actual number of self-generated reports in addition to the total number of reports (including those that were not self-generated). In addition, please provide a break-down of the self-reporters by age.

Snap is providing the total number of NCMEC reports submitted for 2021-2023 as well as a breakdown of reports that were initiated by user reporting. We do not have a breakdown of user reports by age.

| Year | Global NCMEC Cybertips | Number of Global NCMEC Cybertips that were initiated by user reports |
|---|---|---|
| **2023** | 690,000 | 234,600 |
| **2022** | 551,000 | 38,570 |
| **2021** | 512,000 | 97,280 |

**8.** What is Snap's policy or protocol with respect to law enforcement accessing user data and subsequent notification to users of law enforcement accessing their data?

We do not notify users when law enforcement provides a nondisclosure order or when we believe an exceptional circumstance exists, such as cases involving child exploitation, or the threat of imminent death or serious bodily injury, such as the sale of fentanyl. When law enforcement does not provide a nondisclosure order, we will follow up to see if they plan to obtain a nondisclosure order before we take steps to notify the implicated user.

**a.** Do certain crimes such as drug trafficking or child exploitation affect Snap's decision to notify a user whose data is accessed by law enforcement?

Yes, we waive our user notice policy when we believe an exceptional circumstance exists, such as cases involving child exploitation, or the threat of imminent death or serious bodily injury, such as the sale of fentanyl.

**b.** Do certain requests such as a subpoena or search warrant affect Snap's notification protocol? If so, what are they?

Snap's user notice policy does not differ from what is stated above for subpoenas or search warrants.

**c.** If Snap does notify users of law enforcement accessing their data, why does Snap find this necessary?

We do not provide user notice when providing notice is prohibited by a court order or by other legal authority; or when we believe an exceptional circumstance exists, such as cases involving child exploitation, or the threat of imminent death or serious bodily injury, such as the sale of fentanyl. When law enforcement believes that critical evidence would be erased as a result of user notification, they commonly seek and are granted a non-disclosure order. Due to the use of non-disclosure orders and Snap's policy to exempt cases involving the exceptional circumstances noted above, fewer than 5% of account holders for whose accounts data was sought were notified of legal process between June and December 2023.

In these circumstances where law enforcement does not believe that there is a risk that evidence will be destroyed and thus has not sought a non-disclosure order and where no exceptional circumstance exists based on the vulnerability of the victim or threat of imminent harm, we allow affected users a period of time to challenge the legal process in court.

**9.** The National Center for Missing and Exploited Children has indicated that reports from social media companies tend to lack actionable information causing law enforcement to be burdened with incomplete information. How comprehensive are Snap's reports to NCMEC? What challenges is Snap experiencing on the collection of user data and other information to include in its reports to NCMEC? What actions is Snap taking to make its reports more comprehensive and useful to law enforcement?

The safety of our Snapchatters, and specifically child safety, is a top priority for Snap. Child sexual exploitation is abhorrent and illegal, and we act quickly when we identify such conduct. Snap's CyberTips submitted through NCMEC's API are comprehensive and include data in the fields provided by NCMEC through its submission API. Snap is regularly in touch with staff from NCMEC and requests feedback regarding CyberTips submitted to NCMEC. When NCMEC raises questions about particular CyberTips or Snap's processes, teams within Snap quickly review and, as appropriate, make changes to our NCMEC submissions. In the past year,

Snap has made numerous changes to our NCMEC submissions processes based on this regular feedback from NCMEC, as well as from members of law enforcement charged with investigating these horrific crimes.

**10.** The CyberTipline estimates that nearly half of the reports from Snap are lacking essential information, and most critically, child victim identifier information.

Snap's systems are designed to include child victim identifier information (such as the victim username, email address, and phone number) whenever appropriate under Snap's policies. Certain CyberTips do not contain this information by design because there is at times no party to list in the "victim" category. For instance, the most common scenario is when a report implicates a reporting adult user and a reported minor user who is purportedly advertising their own sexual content for sale (in that case, the minor is the reported party, so we do not separately populate their information in the victim fields). The same is true if two adults share CSAM that is proactively detected – in that instance Snap does not know the identity of the child victim.

We endeavor to make all Snap CyberTips actionable by including available relevant information and we actively seek out feedback from NCMEC and members of law enforcement in furtherance of that goal. We also include victim account information when available and in scenarios in which the victim is an account holder.

> **a.** Of the reports submitted to NCMEC by Snap, how many of them lack information identifying child victims?

Not every CyberTip includes victim information. For example, when two adults share known CSAM, the victim identity may be unknown and thus would not contain information identifying the child victim. In all instances in which we become aware that a report incorrectly omits victim information, and we are in possession of such information, we work to retract and resubmit those CyberTips with the information included.

> **b.** Why can't Snap provide child victim identifiers to help law enforcement rescue children who have been exploited on its platform?

Snap does provide child victim identifiers, when appropriate, in CyberTip reports along with additional information, such as the email or phone number associated with the account. We continue to seek input from NCMEC and law enforcement about the actionability of our CyberTips and how to improve them.

**11.** Saved CSAM images and screenshots, derived from conversations between child predators and exploited children operating their child accounts allow child predators to spread CSAM. For conversations involving child accounts, is it possible to disable a recipient's ability to save or screenshot CSAM messages?

When Snap identifies CSEAI on our service, we remove the content and enforce against the relevant account, and we report the account to NCMEC. While it is not possible to disable a recipient's ability to save or screenshot particular messages, Snapchat notifies a user if another party to a conversation has saved or screenshotted any part of their conversation. The ability to screenshot is a functionality that exists at the operating system level rather than the app-level.

**Sen. Josh Hawley (R-MO)**

**1**. Do you allow your children to use social media? If so, please explain under what conditions.

Only one of our children is 13 years old, the minimum age for many online services. We do not allow him to use social media. We allow him to use Snapchat.

**2**. Do you believe that children under the age of 18 should be allowed to use social media?

Yes, although we believe their experience should be different from an adult experience, which is why we offer a different content experience for teens than adults and also give parents and guardians visibility into their teens' Snapchat experience through Family Center.

**3**. How many individuals does your company employ in Trust & Safety?

We have over 2,200 employees and contingent workers that support safety efforts at Snap. The majority of these personnel support trust and safety and content moderation.

**4**. How many individuals does your company employ to review content for so-called "misinformation," "disinformation," or "malinformation"?

Snap does not employ individuals for the dedicated purpose of reviewing content relating to any particular type of harm, such as various forms of information manipulation. Any potential violations of our Community Guidelines are reviewed by our content moderation teams and/or trust and safety teams.

**5**. How many dollars per year does your company spend on salaries for Trust & Safety officers?

At least 20%, including both employees and contingent workers, of our company works on safety – including our moderation teams, trust and safety teams, law enforcement operations teams and more. For 2023, total spend on salaries for all team members working on trust and safety, product safety, safety engineering, and content moderation and review is approximately $135 million.

**6**. Do you believe that the algorithms your company has developed to sort users' feeds are protected by Section 230 of the Communications Decency Act of 1995? If so, please explain why.

Yes, we believe Section 230 covers the algorithms used to rank and display content to users. This interpretation is supported by judicial rulings from several federal courts of appeal around the country.

**7**. Do you believe that the algorithms your company has developed to sort users' feeds are expressive speech protected by the First Amendment to the U.S. Constitution? If so, please explain why.

Yes, courts have consistently held that First Amendment protections apply to the way online services disseminate or curate third-party content.

**8**. Is your company a member of a party, an amicus, or a member of an amicus in NetChoice, LLC v. Paxton, No. 22-555 (U.S.), or did your company provide any funds or donations to any party or amicus in that case? If so, please describe the amount of funds or donations made and the context.

Snap is a member of NetChoice. Snap did not contribute to any party or amicus in support of the NetChoice LLC v. Paxton case.

**9**. Do you believe that the First Amendment to the U.S. Constitution precludes Congress from enacting legislation holding social media companies liable to users for torts they commit?

Yes. Snap supports thoughtful regulation designed to minimize harms that may result from the use of online services. Snap does not believe that, consistent with the First Amendment, liability can attach to companies whose only role in a tort that one user commits on another is the transmission of information and facilitation of communication. Attaching liability to online services that are conduits of such speech would force online services to drastically cut back on the ability of users to communicate online, with a significant chilling impact on constitutionally protected speech.

**10**. Do you believe that companies can be trusted to develop artificial general intelligence (AI) through open-source methods?

Snap does not open-source our artificial intelligence technology. We believe it is important to monitor AI systems and their outputs to ensure they are being used and evolved safely.

**11.** Do you believe the government should play a role in licensing certain artificial intelligence technologies, such as generative AI products?

Snap believes that a risk-based approach to technology policy is appropriate. There may be narrow, high-risk categories of AI technology for which a licensing regime could prove beneficial; however, detailed information would be needed to assess the virtue of such an approach.

**12.** Do you believe that artificial intelligence represents an existential threat to humanity?

Artificial intelligence represents a field of technology that is yielding powerful, transformational advancements in human potential. Like other paradigm-shifting scientific achievements, its potential for harm merits serious attention, just as its potential benefits should inspire steadfast cultivation.

**13**. Do you think that the development of large language models by Microsoft, Google, Meta, and other large companies raises antitrust concerns?

Snap believes competition is critical for safeguarding American technological leadership in the world. Large language models are expensive to develop which may make it difficult for smaller companies to access and benefit from their potential.

**14.** What steps does your company take to make transparent the algorithms by which users are censored, shadow banned, or demonetized?

We take several steps to ensure that our content moderation policies and practices are transparent to our users. First, we publish our acceptable use policies for public review, which include our Community Guidelines, our Advertising Policies and Commercial Content Policies, and our Content Guidelines for Recommendation Eligibility. We also provide Snapchatters with an overview of how we moderate content, enforce our rules, and enable users to appeal our decisions. Through these resources, we aim to provide transparent guidance about what we do and do not permit to afford users a clear understanding of how we distribute user generated content on our platform.

Second, we provide notice to our users, and opportunities to appeal moderation decisions. When content is removed we provide notice to our users that it has been deleted for violating our Community Guidelines. We also inform users when content is restricted from broad distribution in Spotlight or on their Public Profiles, and tell them why. When an account is deleted for violating our Community Guidelines, the user is notified and afforded an opportunity to appeal.

**15.** What steps does your company take to ensure that your company is not disproportionately targeting or censoring conservative voices?

We apply our Community Guidelines consistently, regardless of the account owner. Those guidelines expressly note that our rules "apply to all content (which includes all forms of communication, like text, images, generative AI, links or attachments, emojis, Lenses and other creative tools) or behavior on Snapchat — and to all Snapchatters." The political affiliation of users is not assessed at any stage of our content moderation or policy enforcement processes.

**16**. Do you condemn Hamas' terrorist attacks on the State of Israel on October 7, 2023?

Yes.

**17.** What role do you believe social media companies have in promoting or limiting public speech regarding the events of October 7, 2023?

We have a zero-tolerance policy for hate speech and discrimination, and we condemn content that encourages dangerous and illegal behavior, like encouraging violence. We deliberately designed Snapchat differently than traditional social media services and don't facilitate unvetted content going viral or being algorithmically promoted to large audiences. Instead, we vet content before it can be recommended to a large audience, which helps protect against the distribution of potentially harmful or dangerous content.

In response to the events of October 7, 2023, we mobilized a dedicated cross functional team, including Trust & Safety, Content Moderation, Engineering, Policy, Legal, and Global Security, to take action on content that violates our Community Guidelines. These guidelines apply to all content, and prohibit malicious disinformation, hate speech, terrorism, violence (including graphic violence) and violent extremism.

**18.** What investments has your company made in anti-CSAM technology?

The sexual exploitation of any young person is horrific, illegal and against our policies. We prevent the distribution of CSAM in three key ways:

- We use cutting edge technology – PhotoDNA and CSAI Match – to proactively identify known CSAM photos and videos uploaded to Snapchat and report them to NCMEC.
- When we enforce against illegal and abusive content, we retain it for an extended period so that it is available if law enforcement want to follow up with a valid legal request.
- We take urgent action when we receive reports of CSAM, generally responding within 15 minutes.

We are actively exploring multiple privacy-respective ways of utilizing technology like Google's Content Safety API to detect novel CSEAI. We are exploring our own approaches as well, partnering with experts and organizations to potentially train our own bespoke image classifiers for photos, videos, and synthetic imagery. We will continue to iterate with our industry peers and expert organizations on ways to address these challenges.

**19.** Have you read the Fifth Circuit's opinion in Missouri v. Biden, No. 23-30445?

Yes.

**20.** Do you dispute any factual findings in the Fifth Circuit's opinions or the district court's opinions?

Neither the Fifth Circuit nor the district court opinions had any factual findings concerning Snap or Snapchat. Snap is not in a position to dispute any of the factual findings with respect to the interactions between the federal government and other online services.

**21.** Does your platform continue to receive requests from federal agencies to censor or promote certain content?

No, we have not received requests from federal agencies to censor or promote particular types of user content. We apply our Community Guidelines consistently, and they are publicly available here.

**22.** What steps do your platforms take to verify and enforce age restrictions?

When registering a Snapchat account, users are required to accept Snap's Terms of Service, acknowledge the Privacy Policy, and provide their date of birth. Users need to be at least 13 to create a Snapchat account, and the registration process fails if a user is under the age of 13. If we become aware that a Snapchat user is under the age of 13, we will terminate that user's account and delete the user's data. We also implement a safeguard that prevents younger Snapchat users with existing accounts from updating their birthday to an age of 18 or above. Specifically, if a Snapchat user between the age of 13 to 17 attempts to update their year of birth to reach an age over 18, we will prevent the change.

**23.** In cases where a child's safety is at risk, how does your company collaborate with law enforcement? What information or assistance is provided?

Supporting law enforcement in a timely manner is a priority for our Law Enforcement Operations team, which responds to most legal processes within two to three weeks. In the event we receive an emergency disclosure request, involving an imminent danger of death or serious injury, our team usually responds within 30 minutes. In addition to supporting all valid requests from law enforcement, our team works to proactively and quickly escalate to law enforcement any content involving imminent threats to life. For example, in 2023, we escalated more than 3,000 imminent threat situations to law enforcement.

**24.** Do you believe there is any expressive value in CGI or AI generated CSAM?

No.

**25.** Do you believe that CGI or AI generated CSAM is protected by the First Amendment to the U.S. Constitution?

Our tools are designed to prevent people from creating CGI or AI generated CSAM. We have not analyzed whether such material is protected by the First Amendment.

**26.** What measures does your platform take to ensure that children only see age-appropriate advertisements?

In accordance with the law, we limit distribution of certain ads to certain groups (e.g. only targeting alcohol ads to 21+ in the US). For Snapchatters aged 13 to 17, we do NOT allow ads for things like prescription medication, gambling, alcohol, tobacco, sexualized content, weight loss products or dating apps. All ads on Snapchat must adhere to our Advertising Policies, Community Guidelines and Terms of Service. We have a moderation team that reviews ads for compliance, including ads that are reported by our community.

**27.** Will you commit to setting up a compensation fund for those who have been harmed by your platform?

We will continue to invest in trust and safety initiatives and work with law enforcement to hold bad actors accountable for their actions. We're exceedingly grateful to those who, under horrific circumstances, have shared their experiences with us, and those stories drive us to continuously improve. The steps we've taken as a company can't reverse the tragedies they've experienced, but we all have the same goal – to keep young people – and, indeed, all people – safe when using our service.

**28.** How many sales of fentanyl are transacted through Snap each year?

No fentanyl sales are transacted through Snapchat. There is no user-to-user marketplace feature on Snapchat, and Snapchat does not have a system for payments between Snapchat users. We work to prevent users from communicating about drug sales on Snapchat by proactively detecting drug-related content and blocking dealers from using our service.

This conduct is illegal and we invest a significant amount of resources in attempting to make Snapchat an inhospitable service for drug dealers to communicate about drug deals.

**29.** What steps is Snap taking to eradicate traffic of illegal narcotics on the platform?

Snapchat has been working for years to remove drug dealers from our service. We block drug-related search terms and respond to those queries with educational content. We proactively detect and remove drug-related content including powders and pills. When we enforce against illegal and abusive content, we retain it for an extended period so that it is available if law enforcement wants to follow up with a valid legal request, and we also make proactive referrals for prosecution. We've collaborated with other services and with NGOs to support some of the country's most significant public education campaigns so that people know one pill can kill. We launched signal sharing with Meta because we know criminals use multiple services and sharing

signals can help us keep people safe. We also support a legislative approach, including the Cooper Davis Act, which we have supported since its inception.

**30.** What steps is Snap taking to eradicate child pornography on the platform?

As to Snap's efforts to combat child pornography specifically, please see response to question 18.

**31.** Why did Snap seek sanctions in case No. 3:22-cv-619 in the Southern District of California against plaintiffs who alleged that they were underage victims contacted by adult male perpetrators and groomed on your platform?

Snap sought sanctions against the attorneys who filed that case because the complaint contains several clear falsehoods about how Snapchat works. For example, the complaint falsely alleged that Snapchat's friend suggestion feature, Quick Add, would suggest friends based solely on geographic proximity or shared interests, trying to make the Court believe that a child predator could get friend recommendations for minors on Snapchat simply by loitering near a school or feigning an interest in topics that appeal to minors. That is not how Quick Add works. Quick Add does not recommend users based merely on shared interests or because users may be near a similar location like a school or a park. Quick Add instead primarily makes friend suggestions based on a user's social graph, such as having mutual friends in common. The purpose of QuickAdd is to connect a user with other Snapchat users they already know, not strangers.

The complaint contained many other demonstrably false accusations, as well. It is sanctionable conduct for attorneys to put known falsehoods in their complaints in an attempt to survive a pleading challenge. Because Snap is not able to contest the factual allegations in Plaintiffs' complaint on a motion to dismiss, Snap had to file the motion for sanctions seeking to have the false paragraphs removed from the complaint to correct the record. The court concluded that the Plaintiffs' allegations were "tenuous and confounding," that other allegations were "a stretch, suggestive of sloppy drafting," and that some of the allegations "lack apparent basis in fact."

**32.** Does Snap have access to and provide copies of users' direct message communications to federal law enforcement upon request?

Upon receipt of valid legal process which authorizes such a disclosure, Snap will provide all communications content in our possession for the implicated account.

**33.** How does Snap test new products (such as My AI) to determine whether they are safe and healthy for children?

We prioritize the safety and wellbeing of our community, making it a core aspect of our product development. Snapchat features, especially those incorporating AI, undergo a meticulous review process. This involves a rigorous evaluation based on our Safety and Privacy by Design

principles, ensuring that aligns with our commitment to user safety. MyAI is powered by OpenAI's technology, and we've added extra safeguards to help our community have a positive and age appropriate experience.

Before a person can use My AI, they receive a message from us making clear it's a chatbot, that it has limitations, and that we treat the data in these messages differently than conversations with human friends – this helps us strengthen the overall experience, make improvements when the chatbot responds incorrectly, and enhances our protections. We programmed My AI to abide by our Community Guidelines, and to consider a Snapchatter's age group in its responses. We pause a person's access to My AI if they repeatedly try to misuse it.

We also have rolled out more controls for parents through our Family Center tool. Through Family Center, parents have visibility into when their teen is chatting with My AI, and have the option to restrict their teen's access to My AI.

We regularly analyze My AI's responses so we can keep improving it – and continue to find that only a small percentage (0.01%) are "non-conforming," meaning they don't adhere to our policies. A common example of this is when a user asks a question that includes an inappropriate word (sometimes in an attempt to "trick" My AI) and My AI repeats that inappropriate word in response.

**34.** Has Snap conducted internal studies on the psychological effects of filters on users' self-esteem and body image? If not, why not?

Snap has conducted research on filters relating to a range of topics. For example, Snap has conducted research into how users engage with lenses and, in the course of those studies, participants provide a range of responses describing what they enjoy and don't enjoy about those lenses. Snap then uses the collective feedback to inform product development.

**35.** What efforts has Snap made to educate users about the potential impact of excessive filter usage on body image?

It is worth noting that the majority of lenses on Snapchat are intended to be lighthearted and silly filters where users can turn themselves into a hot dog, Halloween character, or other fun creative persona. And when someone elects to use a lens, there is an indicator to other Snapchatters that the image was created with a lens, empowering the recipient to understand how the visual effects have been achieved.

As part of our overall effort to prioritize the mental health of Snapchatters, in 2020, we launched Here For You, a proactive in-app support system for Snapchatters focused on mental health and well-being. Here for You surfaces resources from expert organizations when Snapchatters search on a range of mental health-related topics, including eating disorders, anxiety, stress, depression,

hate speech, bullying, suicidal thoughts, and more. We partner with the National Eating Disorders Association (NEDA) and the National Alliance for Eating Disorders (The Alliance), whose resources appear in the tool.

**36.** Does Snap monitor user behavior to identify potential signs of negative psychological effects related to filter use?

We have Organic and Community AR Guidelines for accepting Lenses into the app. While they do not identify rejecting Lenses for potential signs of negative psychological harm, we do highlight the following policies for Organic Lenses:

- We design every Lens with race, gender, ethnicity, and cultural norms in mind. We leverage our ever-growing diverse training datasets, as well as feedback from community members to do this.
- If a Lens does not resonate with our community, as expressed through a high ratio of user reports, we take that feedback into consideration and will re-review the Lens with a goal to leave as-is, modify, or remove.
- We consider current and historical global events when releasing a Lens, and delay or deny amplification to Lenses that may be deemed insensitive due to broader social occurrences throughout the world
- Lenses should not change your skin tone to mimic a different ethnicity or race
- We do not modify facial or other features in a way that evoke racial, ethnic, cultural or religious stereotypes or stigmatized disabilities
- We present religious and cultural iconography in a respectful manner, with feedback solicited from internal and external subject matter experts. This means we are especially thoughtful around holiday or event-based content, including the geography in which a Les will launch.
- We ensure that a Lens is not deceptive. We use signifiers and watermarks where there may be questions of creative authenticity
- We test Lenses on photos/videos of and in real life settings with diverse groups of people to accurately enforce our policies

Community Lenses submitted by our users are monitored, and rejected, for the following reasons related to potential impact on users:

- Body shape or size
    - Proportion changes that emphasize sexualized body parts
    - “Fat-shaming”
    - Realistic imitations of eating disorders
- Facial Features
    - Face swaps (“deep fakes”) that could be mistaken as authentic (because of seamless quality without a signifier or watermark)

- Intentional racial or ethnic stereotypes
- Mimicry of real-life medical conditions, disabilities, stigmatized ailments, or specifically imitating the effects of an eating disorder

When our Trust & Safety team recognizes a Snapchatter in distress, they will forward self-harm prevention and support resources, and notify emergency response personnel as appropriate. The resources that we share are available on our global list of safety resources, and these are publicly available to all Snapchatters. We have also developed a Safety and Privacy Hub that provides additional details on our Safety and Privacy by design approach, as well as resources for reporting safety concerns and guidance for staying safe on Snapchat.

**37.** When users exhibit signs of body dysmorphia, eating disorders, or related issues, what measures does Snap have in place to provide support or resources?

We integrate safeguards and tools we use across Snapchat, including blocking results for many harmful topics and providing in-app resources which show Snapchatters resources from expert partners when they search for content related to eating disorders, mental health, anxiety, depression, bullying and related topics. Our Community Guidelines strictly prohibit the glorification of eating disorders and self-harm, gratuitous violence, bullying and harassment, or sending a Snap with the intention of hurting or harming another person.

As part of our overall effort to prioritize the mental health of Snapchatters, in 2020, we launched Here For You, a proactive in-app support system for Snapchatters who may be experiencing a mental health or emotional crisis by surfacing resources from expert organizations when Snapchatters search on a range of mental health-related topics, including eating disorders, anxiety, stress, depression, hate speech, bullying, suicidal thoughts, and more. We partner with the National Eating Disorders Association (NEDA) and the National Alliance for Eating Disorders (The Alliance), whose resources appear in the tool.

When our Trust & Safety team recognizes a Snapchatter in distress, they will forward self-harm prevention and support resources, and notify emergency response personnel as appropriate. The resources that we share are available on our global list of safety resources, and these are publicly available to all Snapchatters. We have also developed a Safety and Privacy Hub that provides additional details on our Safety and Privacy by design approach, as well as resources for reporting safety concerns and guidance for staying safe on Snapchat.

**38.** What is the total dollar value of all drug deals facilitated by Snap since its inception?

Snapchat does not facilitate drug deals. There is no user-to-user marketplace feature on Snapchat, and Snapchat does not have a system for payments between Snapchat users. We proactively detect and remove drug-related content and block dealers from using our service.

**Sen. Mike Lee (R-UT)**

**1**. The 2022 Thorn Report identified Snapchat as the #1 platform where most minors (21 percent) reported having an online sexual encounter with someone they believed to be an adult (14 percent). Amongst minors who share self-generated CSAM, 52 percent say they do so with people they only know from online interactions. What is Snapchat doing to cease being the preferred platform for predators to sexually exploit children?

We know that Snapchat is used by the vast majority of American teenagers, which we believe contributes to the prevalence of these interactions when compared to other services which are not used as frequently by teenagers. Accordingly, we have an enormous responsibility to help keep our community safe. We've designed Snapchat to make it difficult for predators to find and interact with teens.

There are no public friend lists, and by default teens must have proactively added someone as a friend or have them in their contact book to receive a direct message from a user. That's different from text messaging where anyone who has your phone number can get in touch. We also have extra safeguards to block predators from being able to find and search for teens, and to warn teens if an adult tries to contact them who isn't a mutual friend or existing phone contact.

In addition, we are investing resources in learning about the techniques that these predators use, so that we can identify possible sexually exploitative conduct and quickly take action against the accounts. When we disable accounts for sexual exploitation and grooming behavior, we also take steps to block the associated device from creating another account on our platform. Predators' techniques are always evolving, which requires continued focus on the part of all platforms.

We also offer easy reporting mechanisms so teens can get help quickly, and we typically respond to these reports in under an hour.

**2**. Snapchat restricts certain content from accounts that belong to minors. However, the only age verification measure that Snapchat undertakes to ascertain the age of its users is asking new users to enter their birthdate when they open an account. How do you prevent minors from lying about their age when creating an account?

We cannot prevent minors from lying about their age. We do not want people under the age of thirteen to use Snapchat, and if we determine that an account is used by someone under thirteen we remove the account from our service. We strongly recommend that parents or caregivers who provide a smartphone to children under the age of thirteen utilize the operating system-level parental controls to set the child's age accurately and restrict the downloading of apps that are not intended for children.

**3**. Digital sextortion is a growing epidemic on all social media platforms. The majority of victims of sextortion were approached by predators on your platform. You have increased the number of employees tasked with child safety, and you automatically report suspected grooming to NCMEC. How do you ensure that these predators cease contacting minors? How do you catch these situations before a predator attempts to get the minor to move to another platform?

We are very much aware and focused on the growing rise in financially motivated "sextortion" — where criminals pose as young people and trick victims into sending compromising images. This conduct is illegal and abhorrent, and we take active steps to identify and prevent such exploitation as well as empowering users to identify and report suspicious contact.

We combat this criminal activity by:

- Making it difficult for strangers to search for, find, or contact teens.
- Warning teens if they receive a friend request from another person who isn't a mutual friend or phone contact.
- Keeping friend lists private and preventing teens from having public profiles — which helps prevent criminals from using Snapchat to target a teen's friends
- We proactively detect accounts attempting to engage in sextortion and disable them. When we remove sextortion-related content, we also retain it for an extended period of time in case law enforcement wants to follow up with a valid legal request.
- We've added an in-app reporting option specifically for sextortion ("They leaked/are threatening to leak my nudes.") to make it easier for our community to report such abuse to us. When we receive such a report, we take action quickly – usually within 30 minutes.
- We also educate teens about the dangers of this type of crime and urge them to use our in-app reporting tools.

This is very important because young people may feel afraid to report the problem to their parents or caregivers.

**4**. How does Snapchat inform parents when a child is exposed to sexual material? How does Snapchat inform parents when their child is the target of grooming?

Snap's parental resource, Family Center, is designed to spark meaningful conversations between parents and teens about who the teen is communicating with on Snapchat and the content the teen is viewing. For parents and teens who are part of Family Center, parents can see, among other things, who their teen is friends with and who they have been communicating with over the last week, without compromising the teen's privacy by disclosing the content of any messages. The parent can also set content controls. If a parent is concerned about a particular friend, the parent can easily report the account to Snapchat for review. At its core, Family Center seeks to

spark dialogue between teens and their caregivers about staying safe on the app and online generally.

**5**. Besides scanning uploaded pictures for known CSAM, what other measures is Snapchat taking to prevent minors from sharing self-generated CSAM with others?

Snap engages in awareness-raising and education about the consequences of creating self-generated CSAM. We make available in-app a channel called "Safety Snapshot," which includes an episode about sexting and sharing self-generated CSAM. The episode seeks to speak to teens in a relatable language and style, and offers links to helpful resources. It was reviewed and approved by experts at the National Center for Missing and Exploited Children (NCMEC) prior to release.

In addition, we participate in NCMEC's Take It Down program, which allows minors to generate a digital fingerprint (called a "hash") of selected images(s) and video(s) directly on their device (i.e., cellphone, computer, tablet). Participating companies, including Snap, can then use those hashes to detect matches and remove imagery that violates our Community Guidelines. We help to evangelize the availability of the Take It Down program to our community in communications with under-18 sextortion victims, encouraging them to leverage the service. We will continue to iterate with our industry peers and expert organizations on ways to address these challenges.

We are also actively exploring multiple privacy-protecting ways of utilizing technology like Google's Content Safety API to detect novel CSAM. We are exploring our own approaches as well by partnering with experts and organizations to potentially train our own bespoke image classifiers for photos, videos, and synthetic imagery. We will continue to iterate with our industry peers and expert organizations on ways to address these challenges.

**6**. Snapchat does not monitor the content of conversations between users, which contributes to rampant illegal activity on your platform. This includes drug trafficking, weapons trafficking, and child sexual exploitation. What are you doing to eliminate these types of exchanges? Should you do more?

Snap invests a significant amount in safety and combating harms, and more than 20% of our team works on safety-related matters. For example, Snapchat has been working for years to remove drug dealers from our service. We block drug-related search terms and respond to those queries with educational content. We proactively detect and remove drug-related content including powders and pills. When we enforce against illegal and abusive content, we retain it for an extended period so that it is available if law enforcement wants to follow up with a valid legal request, and we also make proactive referrals for prosecution. We've collaborated with other services and with NGOs to support some of the country's most significant public education campaigns so that people know one pill can kill. We launched signal sharing with Meta because we know criminals use multiple services and sharing signals can help us keep people safe.

We support a legislative approach to helping combat drug activity online, including the Cooper Davis Act, which we have supported since its inception. Additionally we are proud to support the Kids Online Safety Act, which will create standards for all services to protect the privacy and safety of young people online and have already implemented many of its provisions. We are happy to provide additional detail on how we address other severe harms as well.

Snap is aware of no communications service that proactively monitors all of the content of private conversations between users. Telephone service providers do not listen to their customers' conversations looking for evidence of illegality. Email service providers do not read their customers' emails looking for evidence of illegality. The postal service does not open and read letters transmitted by mail looking for evidence of illegality. For Snap to screen private messages looking for evidence of illegality would be a gross invasion of our community's privacy, and we do not believe such monitoring is warranted when the vast majority of our community uses Snapchat to communicate safely with their friends and family.

**7**. Do you intend on employing end-to-end encryption for accounts that belong to minors?

We believe encryption is important in helping people communicate with their friends and family privately and safely, but we do not plan to implement end-to-end encryption in a way that would prevent us from being able to detect known child sexual abuse material or constrain our ability to report such content to the authorities.

**8**. Snapchat Stories are a growing concern among parents, and for good reason. From the inception of that feature, those public stories have been plagued by sexually explicit, degrading, and morally repugnant material. This issue was brought to your attention by the Senate Commerce Committee in October, 2021, and despite promises of increased moderation by Snap, Snapchat Stories continue to host reprehensive material. Why are creators using Snapchat Stories permitted to upload this type of content for public consumption?

We work to ensure that Snapchatters have an age appropriate experience across all surfaces on our app. On Snapchat's public content surfaces — which includes Spotlight and Snapchat Stories (also known as Discover) – we do this in a few ways:

- We moderate content before it can be recommended to a large audience; all content is assessed against our Content Guidelines for Recommendation Eligibility. We have introduced new moderation techniques, as well as safeguards to ensure teen users are age-gated from suggestive content on Discover by default.
- We use automation (such as signal-based detection, machine learning, and keyword lists) to proactively identify and remove certain types of harmful or illegal content upon submission (including CSAM, illicit-drug, and sextortion-related content).
- We work with NCMEC, law enforcement, and industry partners to identify, remove, and escalate harmful content and to remain vigilant against emerging risks and trends.

- For infractions that are less egregious, we use a Strike System to crack down on accounts that repeatedly attempt to share content that violates our Community Guidelines.

We also know parents may have different comfort levels on what types of content their teen can view based on their maturity and family values. Our Family Center tools allow parents to set controls that filter out suggestive or sensitive content from recommendations in Spotlight or Discover.

**9**. In January of this year, a researcher at NCOSE created a fake Snapchat account posing as a 13-year-old. Within ten minutes, that account accessed videos simulating sex acts, men slapping women's barely-clothed rears, strip club promotions, and stories about how men should sexually pleasure women—all through the Snapchat Stories section. How do you permit accounts—that you know belong to minors—to access these types of materials? Why are these stories hosted and promoted by Snapchat? What will you do to put an end to a minor's ability to access these promoted materials?

NCOSE made us aware of these findings, and we immediately investigated. We uncovered an issue in Saved Stories due to a gap in our suggestive filtering logic implementation. As of January 31, that gap was closed. It is important to note that this issue involved suggestive content, not explicit content. We detect and remove explicit content automatically through machine-learning technology. We want all Snapchat users to have an age-appropriate content experience – especially teens – and aim to provide this in a few ways:

- We moderate public content before it can be recommended to a large audience, and have strict content guidelines for what is permitted on Snapchat.
- We use machine learning to proactively find sexually explicit content and accounts, so we can remove them.
- We use a Strike System to crack down on accounts trying to market this content.

We also know parents may have different comfort levels as to the types of content they would like their teens to view based on the teen's age, their maturity level, and their family values. Our Family Center tools offer parents the ability to set controls that filter out even further suggestive or sensitive content. As of 2023, new joiners to Family Center have these Content Controls turned "on" by default.

**10**. The Department of Justice reported that Snapchat's "Suggested Friends" feature provides an avenue for a predator to easily access an entire network of minors. Once one minor accepts the request from a predator, that predator can easily move from one minor's network to another without end. Will you discontinue the Suggested Friends feature for accounts belonging to minors?

Quick Add is a tool that makes it easier to find close friends. We make sure that a young person under 18 is not recommended to another person unless they have multiple mutual friends, meaning they are likely to know them. Quick Add does not recommend users based on shared interests or because users may be near a similar location, like a school or a park. Quick Add instead primarily makes friend suggestions based on a user's social graph, such as having mutual friends in common. The purpose of QuickAdd is to connect a user with other Snapchat users they already know, not strangers.

We also show warnings to teens if someone with whom they do not share a mutual friend tries to chat with them.

**Sen. Alex Padilla (D-CA)**

**1**. In recent years, more companies in the tech sector are offering tools to enable caregivers to have a dialogue with minors in their care about healthy and safe internet activity. An important element in understanding whether these tools are helpful is understanding whether or not these tools are being adopted. You were the only CEO prepared to answer questions about adoption rates, and you shared at the hearing that approximately 20 million teens use Snapchat in the United States, that around 200,000 parents use the Family Center supervision controls, and that 400,000 teen accounts have been linked to a parent's account through Family Center.

**a**. How are you ensuring that young people and their caregivers are aware of these tools?

We are constantly working to educate Snapchatters and parents about the accessibility of tools such as Family Center. We promote Family Center at large online safety conferences and events, as well as smaller gatherings and meetings. We engage with nonprofits and NGOs to help make parent groups and related organizations aware of Family Center, including with influential groups such as the National Parent Teacher Association (PTA) and the American Federation of Teachers. We also invest in search engine optimization advertising, allocating budget to Google search ads so that Family Center information is ranked at the top for parents looking for information on parental tools.

**b**. How are you ensuring that these tools are helpful to both minors and their caregivers?

Prior to Family Center's launch in the U.S. in August 2022, and on several occasions since, we have conducted focus groups with both parents and teens. We also sought feedback and input from more than 40 child safety experts across the globe before Family Center was released. We continue to consult our Safety Advisory Board on updates and improvements to Family Center.

This year, we are excited to launch Snap's Teen Council to hear ideas for continuing to make Snapchat a safer, healthier, and more enjoyable place for creativity and connecting with friends. We appreciate that navigating online can present risks and we want to make sure that young people understand, can recognize, and have the skills to help mitigate those risks. For any teen who participates in our Teen Council, there will also be information for their parents and guardians as well as opportunities to seek their feedback.

**2.** Snap offers a broad range of "user empowerment" tools, and it's helpful for policymakers to understand whether young people even find these tools helpful or are actually adopting them. Additionally, some safety features still put the onus on young people to employ a great deal of judgment about safety.

**a**. How are you ensuring that the burden is not on young people to make adult-level decisions about safety on the services that you operate?

Snap is committed to protecting the privacy and wellbeing of our community, which is why we were the first technology company to endorse the Kids Online Safety Act. In fact we have already implemented many of its provisions such as mandating appropriate default privacy settings, providing safeguards for teens (including additional privacy settings that protect their privacy and offer them control over their experience), offering parental tools, and limiting the collection and storage of personal information.

Protecting the privacy and safety of young people on Snapchat is a top priority, and we did not wait for this bill to be implemented to make these changes.

> **b.** Over the last 4 years, how often have you blocked products from launching because they were not safe enough for children, or withdrawn products from the market after receiving feedback on the harms they were causing?

Our Safety by Design process is structured so that cross-functional teams collaborate in identifying and addressing potential safety risks during the development of a product, often starting at early phases of ideation. Further, beyond safety, there are many considerations that go into product development and decisions about whether to roll out or test products, including technical considerations, resources, testing results, and feedback.

**3.** Existing detection tools for keeping child sexual abuse material from spreading online rely on hashed images of already identified CSAM imagery. There are tools like PhotoDNA and Google's CSAI match tool available for identifying this content. A challenge I hear raised frequently is identifying and removing novel images that have not already been hashed.

> **a.** What would it take to develop better technology to accurately identify and limit the spread of novel CSAM images?

The issue of novel CSAM is a complicated one, but we are actively exploring multiple privacy-protecting ways of utilizing technology like Google's Content Safety API to detect novel CSEAI. We are exploring our own approaches as well, partnering with experts and organizations to potentially train our own bespoke image classifiers for photos, videos, and synthetic imagery. Last year, we joined "Take It Down," NCMEC's program to help remove online nude, partially nude, or sexually explicit photos and videos of minors. We also started evangelizing the existence of, and our participation in, Take It Down in communications with under-18 sextortion victims, encouraging them to leverage the service. We will continue to iterate with our industry peers and expert organizations on ways to address these challenges.

We believe that establishing a legal safe harbor for companies to use CSAM content reported to NCMEC to train machine learning models for novel-CSAM detection is critical. Our team

would be very happy to work with your office — in collaboration with law enforcement and other child safety experts — to help develop a responsible approach to such a framework.

**b.** Are there interventions from Congress that would facilitate identification of CSAM?

Machine-learning tools offer one method by which novel CSAM might be detected. However, companies are barred by current law from using existing CSAM that has been reported to NCMEC in the dataset used to train these tools. Intervention by Congress to permit such use by researchers could help facilitate the creation of effective machine-learning tools for identifying novel CSAM. Our team would be very happy to work with your office — in collaboration with law enforcement and other child safety experts — to help develop a responsible approach to such a framework.

**c.** Based on your company's experience trying to address online sexual exploitation and abuse of minors, are there areas where Congress could be helpful in tackling this problem?

The creation and spread of AI-generated CSAM is quickly evolving and we welcome the collaboration of our industry partners, the government and law enforcement to combat this threat. Congress could help by providing a responsible framework that allows companies to legally and safely test large language models to help detect AI-generated CSAM. Our team would be very happy to work with your office, child safety, experts and law enforcement on how best to do that.

**4**. AI models are making it easier to develop synthetic CSAM. These are either altered images of real people, or wholly synthetic individuals. Policymakers are grappling with what this will mean for law enforcement efforts to hold perpetrators accountable and identify children who are being harmed. In addition to processing a higher volume of Cybertips, investigators will have the added challenge of determining whether the victim in the scenario is in fact a real person. And cases are already being reported where AI generative technologies are being employed to facilitate the grooming and sextortion of minor victims.

**a.** What are you doing to identify and remove AI-generated CSAM on your services?

We prohibit all CSAM on Snapchat, including content that is AI-generated, and use technology safeguards to help ensure this content is not created on Snapchat and, if we identify it, remove it promptly and report it to NCMEC as appropriate.

The creation and spread of AI-generated CSAM is quickly evolving and we welcome the collaboration of our industry partners, the government and law enforcement to combat this threat. One important way we can all get better at preparing for it is to have a responsible framework that allows companies to legally and safely test large language models.

**b.** Do you flag for NCMEC if you perceive the CSAM to be AI-generated?

Yes.

**c.** How prevalent is this kind of content?

We understand the creation and spread of AI-generated CSAM is quickly evolving but Snap has seen very little of this content to date.

**d.** How do you anticipate the rise of AI-generated CSAM will impact NCMEC's ability to process and refer Cybertips to law enforcement?

AI-generated CSEAI, unfortunately, is already proving challenging for NCMEC and hotlines across the globe. Hotline analysts need to closely analyze photos for "tells" (e.g., extra digits, unnatural body positioning) as to whether the images may be wholly AI-generated or include partial depictions of real children. Either way, the process will take longer and delay referrals to law enforcement, as well as take away time from vital review cycles of real illegal imagery.

**e.** Recently, A.I.–Generated explicit images of a major pop superstar were distributed widely online without her consent. That story drew attention to a growing problem over the last year facilitated by AI tools: the generation of deepfake, nonconsensual, sexually explicit imagery of everyday people, including our young people. Will you commit to reporting on the prevalence of this new problem and the steps your company is taking to address this horrendous abuse?

We are committed to reporting suspected AI-Gen CSEAI to NCMEC and are committed to utilizing reliable tools that have been developed to identify it.

**f.** Are there technical or legal barriers that your company has identified preventing thorough redteaming of AI models to ensure they do not generate CSAM?

Evaluating whether models are capable of producing CSEAI is important, yet there is complexity and ambiguity in the legal landscape that makes that difficult. We believe that establishing a legal safe harbor for controlled testing and red-teaming in this area would help to advance child safety, and our team would be very happy to work with your offices — in collaboration with law enforcement and other child safety experts — to help develop a responsible approach to such a framework.

**5.** How companies choose to allocate their resources illustrates their true priorities.

**a.** What percentage of your company's budget is dedicated to addressing child safety on your platform?

Approximately 10% of Snap's overall personnel expense goes toward the core teams that work on safety and content moderation.

**b.** What process or assessment of risk on the platform informed that figure?

Safety is a top priority for Snap. We are constantly evaluating safety risks and reassessing resourcing to ensure that safety issues are appropriately prioritized. More specifically, we take into consideration a combination of the results of our twice annual voluntary Transparency Reports, our internal Harms Prioritization Framework, platform safety metrics and an ongoing survey of the threat landscape to ensure we are dedicating sufficient resources to the most serious risks and potential harms.

**c.** How many layers of leadership separates your trust and safety leaders from you?

Our Chief Security Officer, who reports to me, supervises the Senior Director who oversees the Trust & Safety team and Law Enforcement Operations teams. I also meet directly with the leaders of the Trust & Safety team regularly to review our safety roadmap.

**6.** The companies represented at the hearing have the money and resources to hire teams of Trust & Safety professionals and build bespoke tools to aid with content moderation and integrity work as well as the detection of content like CSAM on their services. This is not necessarily the case for the rest of the tech sector. These are industry-wide problems and will demand industry-wide professionalization and work.

**a.** What is Snap currently doing to support access to open-source trust & safety tools for the broader tech ecosystem?

We work with expert NGOs, the government, and our industry peers to collectively attack this problem, including supporting efforts like NCMEC's "Take It Down" program. Take It Down helps to remove online nude, partially nude, or sexually explicit photos and videos of minors. We also started evangelizing the existence of, and our participation in, Take It Down in communications with under-18 sextortion victims, encouraging them to leverage the service.

In addition, Snap is an active member of the Technology Coalition, a group of 37 tech companies working to end online child sexual exploitation and abuse. Snap has chaired a number of Tech Coalition working groups, including the groups on Tech Innovation, Transparency and Accountability, and Collective Action.

**b.** And if Snap is not doing anything now, will you commit to supporting the development of these kinds of resources?

N/A

**7.** One necessary element of keeping our kids safe is preventing harm in the first place. The National Center for Missing and Exploited Children partnered with the White House, the Department of Justice, and the Department of Homeland Security to create "The Safety Pledge" initiative to combat online child exploitation in September 2020. I understand more government backed public awareness campaigns are being developed.

**a.** Are you partnering with the federal government to distribute health and safety resources to young people?

Yes. Snap was the first private sector company to sign a Memorandum of Understanding with the Department of Homeland Security in support of DHS's upcoming Know2Protect (K2P) campaign. K2P is designed to raise awareness of the risks of child sexual exploitation and abuse online. Snap will provide an ongoing ad grant to DHS for free advertising on the service, and support and promote the campaign among the Snapchat community, parents, and NGOs in a number of ways. Snap is a strong proponent of public-private partnerships that offer a single, galvanizing message and program to raise awareness and educate users about key safety issues.

**b.** What are you proactively doing to educate the minors that use your services about online health and safety?

As part of our overall effort to prioritize the mental health of Snapchatters, in 2020, we launched Here For You, a proactive in-app support system for Snapchatters who may be experiencing a mental health or emotional crisis by surfacing resources from expert organizations when Snapchatters search on a range of mental health-related topics, including eating disorders, anxiety, stress, depression, hate speech, bullying, suicidal thoughts, and more. When our Trust & Safety team recognizes a Snapchatter in distress, they will forward self-harm prevention and support resources, and notify emergency response personnel as appropriate. The resources that we share are available on our global list of safety resources, and these are publicly available to all Snapchatters.

In 2023, we launched four new "Safety Snapshot" episodes in-app to help raise awareness and educate our community about various online sexual-related risks, namely: sexting and nudes, financial sextortion, child sex trafficking, and child online grooming for sexual purposes. Safety Snapshot is our official in-app channel for online safety and privacy advice and guidance. These episodes seek to speak to teens in a relatable language and style, and offer links to helpful resources. All four of the episodes were reviewed by experts at the National Center for Missing

and Exploited Children (NCMEC) prior to release.

We have also provided users on Snapchat with safety messaging regarding the risks of fentanyl poisoning and counterfeit prescription drugs. We developed and made available an in-app education portal called "Heads Up" that distributes content from expert organizations such as Song for Charlie, Shatterproof, the CDC and the Substances and Mental Health Services Administration. If someone on Snapchat searches for drug-related keywords, Heads Up will show relevant educational content designed to dissuade engagement and ultimately prevent harm to our community.

Additionally, in partnership with Song for Charlie, we developed a video advertising campaign that has been viewed over 260 million times on Snapchat, and rolled out a new national filter that raises awareness of the dangers of fentanyl and counterfeit pills and directs Snapchatters to the Heads Up educational portal.

Finally, Good Luck America, a Snap Original news show, produced a special edition series of episodes devoted to educating our community about the fentanyl crisis.

**8.** Sextortion has become increasingly prevalent. Offenders may use grooming techniques or basic trickery to manipulate victims into providing nude or partially nude images of themselves, which are then used to coerce victims into sending more graphic images and videos or pay a ransom. These criminals often threaten to post the images or sensitive images publicly or send them to the victim's friends and family if the child does not comply. From May 2022 to October 2022, U.S. law enforcement and NCMEC witnessed an alarming increase in CyberTips and reports where minors have been sextorted for money. Many young boys, including in California, have committed suicide out of desperation, leaving their loved ones devastated.

**a.** How is your company responding to the growing threat of financial sextortion?

This conduct is illegal and abhorrent, and we take active steps to identify and prevent such exploitation as well as empowering users to identify and report suspicious contact.

We combat this criminal activity by:

- Making it difficult for strangers to search for, find, or contact teens.
- Warning teens if they receive a friend request from another person who isn't a mutual friend or phone contact.
- Keeping friend lists private and preventing teens from having public profiles — which helps prevent criminals from using Snapchat to target a teen's friends.
- We proactively detect accounts attempting to engage in sextortion and disable them. When we remove sextortion-related content, we also retain it for an extended period of time in case law enforcement wants to follow up with a valid legal request.

- We've added an in-app reporting option specifically for sextortion ("They leaked/are threatening to leak my nudes.") to make it easier for our community to report such abuse to us. When we receive such a report, we take action quickly – usually within 30 minutes.
- We also educate teens about the dangers of this type of crime and urge them to use our in-app reporting tools.

This is very important because young people may feel afraid to report the problem to their parents or caregivers.

**b.** What methods are in place to detect and disrupt this type of abuse in real time?

Please see response to question 8.a.

**c.** What kind of user education and awareness are you engaged in?

In 2023, we launched four new "Safety Snapshot" episodes in-app to help raise awareness and educate our community about various online sexual-related risks, namely: sexting and nudes, financial sextortion, child sex trafficking, and child online grooming for sexual purposes. Safety Snapshot is our official in-app channel for online safety and privacy advice and guidance. These episodes seek to speak to teens in a relatable language and style, and offer links to helpful resources. All four of the episodes were reviewed by experts at the National Center for Missing and Exploited Children (NCMEC) prior to release.

**d.** Are you aware of a higher prevalence of sexual extortion or abuse against certain demographics among young users? If not, will you commit to studying this issue and making that kind of information available to improve public education and protection measures?

We have heard from NCMEC and other international safety hotlines, as well as anecdotally, that teen males are often targeted in sextortion schemes. That gender assessment bears out to a degree in our own research. We conducted a deeper dive into sextortion among teens (13-17) and young adults (18-24) as part of our 2023 annual Digital Well-Being Index research that we lead in six counties (Australia, Germany, France, India, UK and US). We asked users about their online risk exposure, among other things, and we asked them about their experiences on all services and devices, not just Snapchat. In that research, among those who reported being catfished and /or hacked, the gender split was 56% male and 44% female.

**9.** Young people need to be at the center of regulatory discussions, and they need to be at the table as products and services they use are designed.

**a.** Are you engaging young adults and youth in your conversations and policies around Trust and Safety on the platform?

Yes. In addition to our Safety Advisory Board, which includes three Generation Z young adults, who are also youth advocates for online safety, at the start of the year we opened applications for Snap's first Council for Digital Well-Being, a pilot program in the U.S. for 13-to-16-year-olds interested in collaborating with Snap to create an even safer and healthier environment for creativity and connection among real friends and family. We plan to select a diverse group of about 15 young people from across the nation for an 18-month-program that will include monthly calls, project work, and engagement with our global Safety Advisory Board. In this first year, selected council members will be invited to Snap's headquarters in Santa Monica, California, for a two-day summit and, in Year Two, we have plans for a more public-facing event featuring council members and showcasing their knowledge and learning. The program will also include a "parent track" for parents, guardians, and chaperones, accompanying the teens to the events.

**b.** How do you proactively keep up to speed with the most pressing issues facing young people online?

Our Safety Advisory Board consists of 18 members, based in 10 countries and representing 11 different geographies and regions. The Board is made up of 15 professionals from traditional online safety-focused non-profits and related organizations, as well as technologists, academics, researchers, and survivors of online harms. These members are experts in combating significant online safety risks, like child sexual exploitation and abuse and lethal drugs, and have broad experience across a range of safety-related disciplines. In addition, we have 3 Board members who are young adults and youth advocates. We selected these members to ensure the Board has ready-access to the all-important "youth voice" and viewpoint; to make certain a portion of the Board includes committed Snapchat users; and to seek to balance professional views with practical perspectives from a core demographic of the Snapchat community.

**10.** For many children, an open dialogue about their internet habits is a best practice, and healthy. But not every child has a parent or a caregiver that is looking out for their best interest. For many kids who are abused, a caregiver or parent is their abuser. Additionally, for many young people, their parents' knowledge of their sexual orientation or their interest in exploring it, fundamentally puts them in jeopardy. Solving for these different needs across our young people at the scale of social media and internet applications is really vital.

**a.** How have you designed your parental tools with this dynamic in mind?

Family Center helps parents get more insight into who their teens are friends with on Snapchat, and who they have been communicating with, while still respecting their teens' privacy and autonomy. It's designed to reflect the way parents engage with their teens in the real world, where parents usually know who their teens are friends with and when they are hanging out, but don't eavesdrop on their private conversations.

**Sen. Thom Tillis (R-NC)**

**1.** Twenty-one is the minimum age to purchase highly regulated adult products such as alcohol, tobacco, and nicotine. Nevertheless, there is a proliferation of user-generated content posted on social media sites featuring underage use of these products. Recently, some have proposed banning these age-restricted products due in part to the user- generated content being available on your respective platforms. Surely, banning these products cannot be the answer. However, we must do more – your company must do more – to shield underage audiences from exposure to this content.

Therefore, as the content moderator of these platforms, what policies do you have in place, and what more can you do, to prevent this type of user-generated content from reaching underage audiences? How do you respond to requests to pull this content from your sites when deemed inappropriate for underage audiences?

We want all Snapchat users to have an age appropriate experience – especially teens – and aim to provide this in a few ways:

- We moderate public content before it can be recommended to a large audience, and have strict content guidelines for what is permitted on Snapchat
- We use machine learning to proactively find sexually explicit content and accounts so we can remove them
- We use a Strike System to crack down on accounts trying to market this content

We also know parents may have different comfort levels on what types of content their teen can view based on their maturity and family values. Our Family Center tools allow parents to set controls that filter out suggestive or sensitive content.

In addition, in accordance with the law, we do limit distribution of certain ads to certain groups to comply with applicable law (e.g. only targeting alcohol ads to 21+ in the US). For Snapchatters aged 13 to 17, we do NOT allow ads for things like prescription medication, gambling, alcohol, tobacco, sexualized content, weight loss products or dating apps. All ads on Snapchat must adhere to our Advertising Policies, Community Guidelines and Terms of Service. We have a moderation team that reviews ads for compliance, including ads that are reported by our community.

**2.** Public reports conclude that drug cartels use social media like TikTok, META, X, Snapchat, and others to plan, organize, and communicate in real-time. These communications coincide directly with criminal activity. What are your companies doing to crack down on cartel coordination? Specifically, in the recruitment of children to commit crimes or assist in the sale/distribution of illicit drugs?

Nothing is more important than the safety of our community. We explicitly prohibit using Snapchat for illegal activity and use proactive detection tools to find this type of content and take it down. We closely collaborate with law enforcement to help prevent abuse on our service and encourage people to immediately report unlawful content, both through our in-app reporting tools and to law enforcement directly.

To help our community easily and quickly report any harmful or illegal content to us, we offer in-app reporting tools, as well as the ability to report via our Support Site or via Twitter. Reporting content is confidential, and allows us to preserve the reported content to investigate it.

As part of our ongoing work to help keep our community safe, we have an in-house Law Enforcement Operations team dedicated to reviewing and responding to law enforcement requests for data related to their investigations. Our global Trust and Safety teams also work around the clock to quickly investigate any reports and take appropriate action.

Snapchat has been working for years to remove drug dealers from our service. We combat this challenge in a number of ways:

- We block drug-related search terms and respond to those queries with educational content.
- We proactively detect and remove drug-related content including powders and pills.
- We preserve drug-related content to make it available for law enforcement and we make proactive referrals for prosecution.
- We've collaborated with other services and with NGOs to support some of the country's most significant public education campaigns so that people know one pill can kill.
- We launched signal sharing with Meta because we know criminals use multiple services and sharing signals can help us keep people safe.

We also support a legislative approach, including the Cooper Davis Act, which we have supported since its inception. Current law strictly limits when Snapchat and other online services can share information about attempts to abuse our services. The bipartisan Cooper Davis Act would establish a new legal framework for information sharing about the sale of fentanyl and other life-threatening drugs, expanding the ability of Snap and other providers to support law enforcement investigations and help bring perpetrators to justice. More can and must be done to combat this national crisis, and we look forward to continuing to work with the Senate to pass this important legislation.

**3.** What steps does your platform take to proactively remove, delist, and ban any posts, users, websites, and advertisements associated with the sale and distribution of fentanyl and other illicit drugs?

Please see response to question 2.

**4**. One area of growing concern is the sale and distribution of fake or counterfeit vaping devices online, particularly in connection with so-called Delta-8 THC. Counterfeit vapes, many coming from China, have unsafe and even potentially deadly chemicals. They have caused hospitalizations and death. What are your platforms doing to combat this problem?

Our Community Guidelines prohibit the illegal promotion of regulated goods or industries, including unauthorized promotion of gambling, tobacco or vape products, and alcohol. Our prohibition against illegal and regulated activities reflects our stalwart commitment to safety across Snapchat. Upholding these rules not only helps ensure our service is not misused for unlawful purposes, but also helps protect Snapchatters from serious harm. To help advance these aims, we partner extensively with safety stakeholders, NGOs, and law enforcement organizations to provide our community with educational resources and to generally promote public safety.

Additional guidance on prohibited illegal or regulated activities that violate our Community Guidelines is available here.

**5**. What are the main impediments your platform encounters in identifying all fentanyl and illicit drug advertisements posted to your platform(s) automatically? Please describe any circumstances in which you do not or cannot apply detection technologies against content transmitted on your platform(s).

Please see response to question 2.

**6**. How many posts, users, websites, and advertisements have you removed, delisted, and banned per year for the sale and distribution of fentanyl and other illicit drugs? How many per year? Have you seen an increase in illicit drugs being advertised to children on your platform(s)?

Last year, we removed approximately 2.2 million pieces of drug-related content and blocked approximately 705,000 associated accounts.

**7**. Are there any other roadblocks or impediments that you face in addressing fentanyl and illicit drug advertisements on your platform(s), and working with law enforcement on such matters? If yes, what are they? If not, how many cases have been transmitted to law enforcement and DEA?

We have long worked with DEA field agents who have been critical partners in our fight against fentanyl. We make proactive referrals to the DEA for prosecution and we work to share intelligence and signals to evolve our detection tools.

**8**. How do you work with organizations, advocates, and experts focused on drug prevention and addiction recovery to adapt your products and operations to keep up with the illicit drug crisis — including working with parents that have lost children due to lethal drugs bought online?

We are committed to educating both Snapchatters and the general public about the dangers of fentanyl. Our ongoing work to combat the nationwide fentanyl crisis includes education for the Snapchat community:

- When it comes to informing our community about the dangers of fentanyl, we meet young people where they are. Over the past two years, we have promoted in-app educational videos and news content warning about the dangers of counterfeit pills and directing them to credible resources from trusted experts. We also have in-app resources tailored to parents to give them greater visibility into their teens' online experiences.
- Our expert partners include the Centers for Disease Control and Prevention (CDC), the Substance Abuse and Mental Health Services Administration (SAMHSA), Community Anti-Drug Coalitions of America (CADCA), Truth Initiative and the SAFE Project.

Our commitment extends to educating the general public:

- We served as a Founding Partner of National Fentanyl Awareness Day to help raise awareness about the urgent crisis.
- As part of our ongoing efforts to raise public awareness, we teamed up with the Ad Council and other tech platforms on an unprecedented public awareness campaign to help people learn more about the dangers of fentanyl, and have partnered with Song for Charlie to reach young people where they are and educate them on about the hidden dangers of fake prescription pills laced with fentanyl. These resources have provided our community with information about the dangers of counterfeit pills and the importance of naloxone as a life-saving medication.

We also want to recognize the many families who have worked to raise awareness on these issues, pushed for change, and collaborated with lawmakers on important legislation like the Cooper Davis Act, which can help save lives.

**9**. What are the total number of meetings that your company has had with parents to address online safety concerns? Can you provide the total number of meetings over the last three years? Please separate this last question's answer by number per year.

Over the last three years, our team has met with more than twenty families to listen to their experiences and address online safety concerns. With some families, we meet more regularly – in some cases – monthly. Parents also serve on Snap's Safety Advisory Board (which meets three times a year) providing a valuable perspective on online safety. In addition, last year, our team participated in several national school safety conferences with an audience of parents, educators, and safety professionals. These included the National Association of School Resource Officers Annual Conference, the Safe and Sound Schools Annual Conference, three National Student

Safety & Security Conference and Workshops, as well numerous direct engagements with parents, school administrators, and school safety officers around the country.

**10**. In 2022, then National Center for Missing & Exploited Children (NCMEC) received over 32 million reports of Child Sexual Abuse Material (CSAM). Reports of online sex crimes to the CyberTipline are growing exponentially year by year. Out of those 32 million reports, how many did your platform submit to NCMEC?

Snap submitted approximately 551,000 CyberTips to NCMEC in 2022, and approximately 690,000 in 2023.

**11**. There is concern that this number is going to fall dramatically this year because of the adoption of end-to-end encryption, not because the problem is going away. How will your company track and address this issue moving forward?

We do not anticipate that our NCMEC reports will decrease this year. We believe encryption is important in helping people communicate with their friends and family privately and safely, but we do not plan to implement end-to-end encryption in a way that would prevent us from being able to detect known child sexual abuse material or constrain our ability to report it to authorities. We proactively scan for and detect known CSAM so we can immediately remove, investigate and report the content and violating accounts to authorities.

**12**. Has your platform seen an increase of suspected online child sexual exploitation- CSAM over the past few years? If so, what do you believe is the driving factor on why it's happening on your platform?

We are very much aware and focused on the growing rise in financially motivated "sextortion" — where criminals pose as young people and trick victims into sending compromising images. Because Snapchat is a platform that is attractive to teens and young adults, our platform is not immune to this trend that's affecting a range of online platforms. This conduct is illegal and abhorrent, and we take active steps to identify and prevent such exploitation as well as empowering users to identify and report suspicious contact.

We combat this criminal activity by:

- Making it difficult for strangers to search for, find, or contact teens.
- Warning teens if they receive a friend request from another person who isn't a mutual friend or phone contact.
- Keeping friend lists private and preventing teens from having public profiles — which helps prevent criminals from using Snapchat to target a teen's friends
- We proactively detect accounts attempting to engage in sextortion and disable them. When we remove sextortion-related content, we also retain it for an extended period of time in case law enforcement wants to follow up with a valid legal request.

- We've added an in-app reporting option specifically for sextortion ("They leaked/are threatening to leak my nudes.") to make it easier for our community to report such abuse to us. When we receive such a report, we take action quickly – usually within 30 minutes.
- We also educate teens about the dangers of this type of crime and urge them to use our in-app reporting tools.

This is very important because young people may feel afraid to report the problem to their parents or caregivers.

**13**. What are some new tools or strategies that your platform has implemented to identify CSAM? How closely does your platform work with NCMEC?

The sexual exploitation of any young person is horrific, illegal and against our policies.

We attack it in three key ways:

- We use cutting edge technology – PhotoDNA and CSAI Match – to proactively identify known CSAM photos and videos uploaded to Snapchat and report them to NCMEC.
- When we remove illegal and abusive content, we retain it for an extended period so that it is available if law enforcement want to follow up with a valid legal request.
- We take urgent action when we receive reports of CSAM, generally responding within 15 minutes.

We are actively exploring multiple privacy-protecting ways of utilizing technology like Google's Content Safety API to detect novel CSEAI. We will continue to iterate with our industry peers and expert organizations on ways to address these challenges.

**14**. What resources or help does your platform provide to victims of CSAM? Does your platform work with local victim groups and professionals?

As part of our overall effort to prioritize the mental health of Snapchatters, in 2020, we launched Here For You, a proactive in-app support system for Snapchatters who may be experiencing a mental health or emotional crisis by surfacing resources from expert organizations when Snapchatters search on a range of mental health-related topics, including eating disorders, anxiety, stress, depression, hate speech, bullying, suicidal thoughts, and more. When our Trust & Safety team recognizes a Snapchatter in distress, they will forward self-harm prevention and support resources, and notify emergency response personnel as appropriate. The resources that we share are available on our global list of safety resources, and these are publicly available to all Snapchatters.

**15**. What are the top technical hurdles your company faces in combating CSAM?

The creation and spread of AI-generated CSAM is quickly evolving and we welcome the collaboration of our industry partners, the government and law enforcement to combat this threat. AI-generated CSEAI, unfortunately, is already proving challenging for NCMEC and hotlines across the globe. Hotline analysts need to closely analyze photos for "tells" (e.g., extra digits, unnatural body positioning) as to whether the images may be wholly AI-generated or include partial depictions of real children. Either way, the process will take longer and delay referrals to law enforcement, as well as take away time from vital review cycles of real illegal imagery, depicting real children that need to be referred and actioned.

**16.** There seem to be competing views on how to regulate algorithms. Some suggest that more transparency is needed, while others want more privacy. Can you provide your perspective on whether more or less transparency is needed when it comes to algorithms?

Algorithms work differently on Snapchat. Unlike other services, we don't apply an algorithm to a feed of unvetted or unmoderated content and there is no rabbit hole of harmful content. Stories and Spotlight, the areas of our service where we apply algorithms to serve content, are closed services where content is moderated and we choose what content is approved for distribution.

Users can manage the type of content they may be served by adjusting their interest categories which are used to serve content we think they will prefer. We believe that our core architecture and design decisions limit the risk of algorithms that are applied to unmoderated feeds driven by engagement signals such as likes and comments. Across our service, we limit the risks of virality, which removes incentives for people to create content that appeals to people's worst instincts, and limits concerns associated with the spread of bad content such as disinformation, hate speech, self-harm content, or extremism.

**17**. Do you believe that large companies and platforms like yours can use algorithms to stifle innovation or small businesses?

We believe that algorithms can and should be designed to promote innovation and small businesses.

**18**. What do you believe is the role of the government in regulating algorithms? What, if any, unintended consequences would there be if Congress gets involved?

Congress plays a critical role in regulating technology and we believe the use of algorithms is a key piece of this oversight. The Kids Online Safety Act, which Snap supports, includes a provision on algorithms to ensure that the safety and well-being of young people is considered when providing algorithmically recommended content. Not all algorithms are intrinsically negative. One unintended consequence of mandating the ability to opt-out of algorithms could result in users seeing content that is not relevant or appropriate to them. We believe that Congress should focus on regulating harmful content and tread carefully when restricting the

algorithms that distribute such content to avoid unintended consequences.

**19**. Are you aware of your platform using surveillance advertisements to target children (anyone under the age of 18) with specific ads? If so, in your opinion, how can this be mitigated?

Advertisers have the ability to target advertising to different age groups as appropriate, and in accordance with the law, we do limit distribution of certain ads to certain groups to comply with applicable law (e.g. only targeting alcohol ads to 21+ in the US). For Snapchatters aged 13 to 17, we do not allow ads for things like prescription medication, gambling, alcohol, tobacco, sexualized content, weight loss products or dating apps. All ads on Snapchat must adhere to our Advertising Policies, Community Guidelines and Terms of Service. We have a moderation team that reviews ads for compliance, including ads that are reported by our community. Snapchat collects information on the types of content Snapchatters engage with and infers their interests in a limited number of non-sensitive interest categories. In our Settings menu, all Snapchatters can change these interest categories to better personalize their experience.

**20**. Beyond surveillance advertisements, are there any other algorithmic-based practices being implemented that are particularly detrimental to children? In your opinion, how can this be mitigated?

No.

**21**. Are you aware of any surveillance advertisements or algorithms that are used to target children, specifically to promote drugs and the sale of narcotics?

No.

**Sen. Sheldon Whitehouse (D-RI)**

**1.** What exemptions from the protections of Section 230 would your company be willing to accept?

Section 230 is a cornerstone of internet safety because it creates a legal mechanism that allows Internet companies to remove harmful content. If Section 230 didn't exist, internet companies wouldn't be able to effectively moderate their platforms to keep people safe. We wish more companies used Section 230 to remove harmful content. We believe that Section 230 could be amended to require, rather than simply allow, companies to remove specific types of harmful content that is not covered by the 1st Amendment, such as CSAM.

**2.** Is it your belief that your company should enjoy absolute immunity under Section 230 from suits like Doe v. Twitter, No. 21-CV-00485-JCS, 2023 WL 8568911 (N.D. Cal. Dec. 11, 2023), no matter the extent of your company's failure to remove reported child sexual abuse material from the platform or to stop its distribution?

Snap submits hundreds of thousands of reports of CSAM to NCMEC each year, and we take these legal obligations seriously. Snap would support legislation to ensure that platforms, upon receiving notice of CSAM on their platform, are obligated to remove that material within a reasonably prompt timeframe.

**Sen. Cory Booker (D-NJ)**

**1**. Trust and safety teams are a vital component in combating the spread of CSAM, hate speech, violence, and other violative content on tech platforms. Despite this, tech companies have time and time again disinvested from their trust and safety team, especially during changes in leadership.

> **a**. How has the size of your trust and safety team changed over the past five years? Please provide numbers for each of the past five years.

Our Safety & Moderation team has grown approximately 190% from 2019 to present.

> **b**. Do your trust and safety teams make submissions to the National Center for Missing and Exploited Children's CyberTipline, or is that a separate unit?

Yes, our Trust & Safety team makes submissions to NCMEC.

> **c**. If it is a separate unit, how many members are on the team and how have those numbers changed over the past five years. Please provide numbers for each of the past five years.

It is not a separate unit.

**2**. The National Center for Missing & Exploited Children's CyberTipline plays an integral role in combating child sexual exploitation. The tipline helps law enforcement investigate potential cases and allows prosecutors to bring justice to victims. While federal law requires your company to report to the CyberTipline any apparent violations of federal laws prohibiting child sexual abuse material of which you are aware, there are many gaps.

> **a**. Is there a standard format your reports to the CyberTipline follow? If so, what is that format?

Yes, we report to NCMEC through the CyberTipline API using the fields NCMEC provides for reporting.

> **b**. Does your company proactively report planned or imminent offenses?

Yes.

> **c**. Does your company proactively report potential offenses involving coercion or enticement of children?

Yes.

**d**. Does your company proactively report apparent child sex trafficking?

Yes.

**Sen. Laphonza Butler (D-CA)**

**1.** Family and parental control tools: I was glad to hear that you have spent time talking with parents and what their families need from your products. I was also glad to hear your companies have a Family Center, or other similar tools, to give parents more insight and control over how their children are using your platforms and apps.

**a.** How do you advertise this feature to parents?

We are constantly working to educate Snapchatters and parents about the accessibility of tools such as Family Center. We promote Family Center at large online safety conferences and events, as well as smaller gatherings and meetings. We engage with nonprofits and NGOs to help make parent groups and related organizations aware of Family Center, including with influential groups such as the National Parent Teacher Association (PTA) and the American Federation of Teachers. We also invest in search engine optimization advertising, allocating budget to Google search ads so that Family Center information is ranked at the top for parents looking for information on parental tools. We are also always looking for ways to make Family Center more easily accessible within Snapchat, to ensure parents have these tools at their fingertips.

**b.** Can you share data on how many Family Center/parental tools users there are in proportion to total minors on your platforms and products?

Approximately 200,000 parents use our Family Center suite of tools, and approximately 400,000 teen accounts have been linked to a parent's account through Family Center representing approximately 0.7% of our 60M global DAU aged 13-17.

**Sen. Chris Coons (D-DE)**

**1**. During the hearing, I asked the five witnesses whether the platform they represented publicly discloses "an estimate of the total amount of content—not a percentage of the overall…but the total amount of content on your platform—that violates" the platform's "policies prohibiting content about suicide or self-harm." I also asked if each platform "report[s] the total number of views that self-harm or suicide-promoting content that violates that policy gets on [each] platform." In response to these questions, you testified while under oath "Yes, Senator. We do disclose." After reviewing Snap's most recent transparency report from December 13, 2023, it appears that your testimony was misleading. First, Snap's transparency report does not disclose an estimate of the total amount of content on Snap's platform that violates the company's suicide and self-harm policy. Second, the transparency report does not disclose the estimated number of views that this violating content on the platform receives. These exclusions stand in direct contrast to your sworn testimony on January 31.

> **a**. Please provide the specific citation to where Snap publicly discloses an estimate of the total amount of content on the platform that violates Snap's suicide and self-harm policy.

We disclose the amount of content that violates the company's suicide and self-harm policy, and we disclose the violative view and viewer rate of such content which is an aggregate measurement of the views and viewers that this content received.

As part of our most recent Transparency Report, covering July 1, 2023 - December 31, 2023, we reported that 24,621 pieces of content and 22,637 unique accounts were enforced for suicide and self-harm, out of a total of 6,216,118 pieces of content and 3,687,082 that were enforced. We also note that this was 0.4% of total content enforced during this time-frame. The Transparency Report is publicly available at the following URL: https://values.snap.com/privacy/transparency.

In addition, our California transparency page links to our California Terms of Service Report, which was published at the time of the hearing. This report, in turn, includes a range of safety-related metrics, including providing the Violative View Rate (VVR) for individual categories of harms, as well as the Violative Viewer Rate which discloses how many viewers saw the content as a percentage of all active users over a period of time, both for the U.S. and globally. The report specifically indicates that suicide and self-harm content enforced by Snap's content moderators in Q3'23 had a violative view rate of approximately 0.000007% (and even less so for automated enforcements). Going forward, we plan to integrate this data into our main, semi-annual Transparency Report for convenience and clarity.

> **b**. Please provide the specific citation to where Snap publicly discloses an estimate of the total number of views of content that violates Snap's suicide and self-harm policy.

Please see response to question 1.a.

**c**. If Snap does not disclose these metrics, why not?

N/A

**d**. Does Snap measure these metrics? If not, why not?

Yes, we measure these metrics, as described in response to question 1.a.

**2**. Snap has previously reported how much content it removes under the platform's suicide and self-harm policy.

**a**. For content that has been removed, does Snap measure how many views that content received prior to being removed? If not, why not?

Yes, we measure this. Please see response to question 1.a for more information.

**b**. For content that has been removed, does Snap disclose how many views that content received prior to being removed? If so, please provide a specific citation to where Snap discloses that information. If not, why not?

We do not currently disclose this metric for each piece of content but rather disclose the violative view rate generally, as described in response to question 1.a. This statistic provides a more intelligible overview of the data, whereas if we were to disclose how many views all content received before they were removed, we'd have thousands of view metrics for each of the thousands of individual pieces of suicide and self-harm content that was enforced. If we extrapolate further, to all of our harms, that would be hundreds of thousands of view metrics, which would not provide meaningful clarity to the actions taken against our content, unlike VVR which provides a more meaningful point of comparison.

**c**. Please provide an estimate of the number of views content that was removed under this policy received in January 2024.

Snap estimates the VVR for self-harm and suicide at approximately 0.00002% for suicide and self-harm content in the U.S during January 2024.

**d**. For content that has been removed, does Snap measure demographic factors about users who viewed the violating content, such as how many times the content was viewed by minors? If not, why not?

Snap measures violative views in the aggregate, via our Violative Viewer Rate, as described in response to question 1.a. The Violative Viewer Rate is the percentage of unique viewers who saw violating content, as a proportion of unique users active throughout the reporting period — but this metric does not currently differentiate between demographics, such as whether the unique user was a minor or an adult, in part because we are committed to reducing violative views of potentially harmful content regardless of users' demographics.

> **e**. For content that has been removed, does Snap disclose demographic factors about users who viewed the violating content, such as how many times the content was viewed by minors? If so, please provide a specific citation to where Snap discloses that information. If not, why not?

No, we do not, for similar reasons to that described in response to question 2.b.

> **f**. Does Snap measure the number of users that have viewed content that was removed under its suicide and self-harm policy multiple times? If not, why not?

Yes, we do, as described in response to question 1.a.

> **g**. Does Snap disclose the number of users that have viewed content that was removed under its suicide and self-harm policy multiple times? If so, please provide a specific citation to where Snap discloses that information. If not, why not?

While we do not disclose specifically the number of users that have viewed a specific piece of content multiple times or, generally, viewed violative content multiple times for reasons discussed in response to question 2.b, we disclose statistics relating to violative views and viewers, as discussed in response to question 1.a.

**3**. Snap utilizes an algorithm to recommend or amplify content to users.

> **a**. For content that has been removed, does Snap measure whether and the extent to which the removed content was recommended or amplified by Snap? If not, why not?

This question assumes that Snapchat algorithmically recommends content that may violate our Community Guidelines. However, on Snapchat's public content surfaces—including Spotlight and Snapchat Stories (also known as Discover)—we moderate content before it can be recommended to a large audience. We also use advanced technology (such as signal-based detection, machine learning, and keyword lists) to proactively identify and remove certain types of harmful or illegal content upon submission (including CSAM, illicit-drug, and sextortion-related content). If content on these surfaces—or elsewhere in Snapchat—violates our Community Guidelines, we at a minimum remove it and it is not eligible for recommendation. If content violating our Community guidelines does slip through our moderation process, we

remove it if it is later reported or discovered, but do not track the extent to which the removed content was recommended or amplified.

> **b**. For content that has been removed, does Snap disclose whether and the extent to which the removed content was recommended or amplified by Snap? If so, please provide a specific citation to where Snap discloses that information. If not, why not?

As discussed in response to question 3.a, algorithmically-recommended content is moderated. In Discover, Publishers and Snap Stars are verified by our internal partnerships team to maintain content quality standards. In Spotlight, content is moderated according to multiple policies, including our Content Guidelines for Recommendation Eligibility, Community Guidelines, and Terms of Service. On both surfaces, content that is reported is reviewed by our moderation team for compliance against our Content Guidelines for Recommendation Eligibility. These intentional design choices minimize the risk of violative content from going viral.

> **c**. For content that has been removed, does Snap measure how many views the removed content received after having been recommended or amplified? If not, why not?

Yes, Snap stores the number of views removed content received before being removed.

> **d**. For content that has been removed, does Snap disclose the number of views the removed content received after having been amplified or recommended? If so, please provide a specific citation to where Snap discloses that information. If not, why not?

No. Given our robust moderation policies, there is a limited amount of violative content that goes viral.

**4**. Does Snap support creating industry-wide transparency requirements to disclose basic safety information, like those included in the Platform Accountability and Transparency Act?

It is our understanding that the Platform Accountability and Transparency Act would allow researchers to access personal data including potentially sensitive personal information. While we are supportive of industry-wide transparency requirements for basic safety information, we take seriously our obligations to protect user data and would not support research access for personal data and sensitive personal information without explicit consent.

**Sen. Ted Cruz (R-TX)**

**Directions**

*Please provide a wholly contained answer to each question. A question's answer should not cross-reference answers provided in other questions.*

*If a question asks for a yes or no answer, please provide a yes or no answer first and then provide subsequent explanation.*

*If the answer to a yes or no question is sometimes yes and sometimes no, please state such first and then describe the circumstances giving rise to each answer.*

*If a question asks for a choice between two options, please begin by stating which option applies, or both, or neither, followed by any subsequent explanation.*

*If you disagree with the premise of a question, please answer the question as-written and then articulate both the premise about which you disagree and the basis for that disagreement.*

*If you lack a basis for knowing the answer to a question, please first describe what efforts you have taken to ascertain an answer to the question and then provide your tentative answer as a consequence of its reasonable investigation.*

*If even a tentative answer is impossible at this time, please state why such an answer is impossible and what efforts you intend to take to provide an answer in the future.*

*Please further give an estimate as to when Senator Cruz will receive that answer. To the extent that an answer depends on an ambiguity in the question asked, please state the ambiguity you perceive in the question, and provide multiple answers which articulate each possible reasonable interpretation of the question in light of the ambiguity.*

**1**. In the last two years, has an employee or commissioner of the Federal Trade Commission (FTC) requested to evaluate or evaluated your data used for training Large Language Models or algorithms or the sources of such data for bias, discrimination, or misinformation?

No.

**2**. In the last two years, has an employee or commissioner of the FTC sought details regarding your company's measures related to filtering or blocking inputs and outputs of a Large Language Model or algorithms?

Yes, the FTC has sought details regarding how Snap trains its chatbot, My AI, to control or modify outputs generated by the chatbot.

> **a**. If yes, has the FTC attempted to coerce or otherwise request you to implement input/output filtering in order to allegedly comply with federal law?

No.

**3**. In the last two years, has an employee or commissioner of the Federal Trade Commission sought to evaluate your company's use of measures, including "prebunking" or "debunking", designed to counteract so called "online misinformation?"

No.

**4**. In June 2022, the FTC released a report titled "Combatting Online Harms Through Innovation." In this report, the FTC discussed how the deployment of AI tools intended to detect or otherwise address harmful online content is accelerating but may never be appropriate as an alternative to human judgment.

> **a**. In the context of protecting children from online harms to what extent does your company rely on automated tools to detect online harm vs. human review? Please be specific.

To help prevent the spread of harmful content on Snapchat, we use a combination of human and automated tools to enforce our Community Guidelines. For example:

- We use automated mechanisms such as machine learning, heuristics-based rule engines and hash matching technologies to proactively detect violative content and accounts, and to take enforcement action. When these mechanisms have high enough confidence they are used to make automated decisions and, when unsure, content and accounts detected by these models are augmented with human review labels to make enforcement decisions.
- We similarly use a combination of automation and human review to approve the content that is recommended on our service.
- We use human review decisions and labels as the source of truth to evaluate the efficacy of our automated mechanisms, perform quality assurance checks and as critical inputs to augment automation.
- We use automated abusive language matching mechanisms to block search results for a wide range of terms related to online harms. In some instances, such as with drug-related terms, we instead redirect Snapchatters to resources from experts about the dangers of fentanyl.

- We use human review processes to fact-check all political and advocacy ads. All political ads, including election-related ads and issue advocacy ads, must include a transparent "paid for" message that discloses the sponsoring organization, and we provide access to information about all ads that pass our review in our Political Ads Library.

**b**. What benefits can AI provide to helping detect and/or stop harmful content to children online?

Automated tools, including AI and Machine Learning systems, represent an important part of our overall approach to moderation. For example, we use machine learning to specifically train models to proactively detect harmful content or to identify suspicious account behavior — for example relating to illicit drug content or distribution. We do this so we can immediately remove such offending content from Snapchat. The ability to improve our proactive scanning capabilities with artificial intelligence is critical to our safety efforts.

**c**. What does a human reviewer provide that an AI or automated tool cannot? Will we always need some measure of human review in assessing online harms to children?

We believe a combination of human review and machine learning or AI technologies provides the most comprehensive approach to moderation. We continue to invest in new machine learning capabilities to improve our proactive detection of potentially harmful content. At the same time, human review is critical to accurately assess and take action on reported or proactively detected content at least until automated machine learning performs on par with human review of the particular type of content. In addition, human review is necessary to label and perform quality assurance on tasks generated by machine learning models. We have actually grown the size of our human review teams significantly in recent years.

**d**. The FTC has sent mixed signals in its enforcement of COPPA. While the Commission emphasizes not over relying on use of automated tools or AI, they have nonetheless found liability for using human review as alternative signaling overreliance on automated tools. What improvements, if any, should Congress make to clarify the legal tension between use of automated detection tools vs. human review?

We believe clearer guidance and consistent enforcement from the FTC on human review and use of automated tools or AI is needed. Additional guidance from Congress providing legislative direction to the FTC to not penalize companies who use human review methods in combination with automated tools would be valuable and ensure that companies who make good faith efforts to keep their service safe are not unfairly punished.

**5**. In 2021, Congress directed the FTC to research and report on how AI can be used positively to detect and combat fraudulent or deceptive content online. Rather than viewing AI as a potential

solution to our online woes, the FTC instead issued a report that read more like an indictment of the technology.

> **a**. Please explain whether, in your view, AI can be used to positively detect and combat fraudulent or deceptive content, including the recent use of deep fakes or other scams to harm consumers.

We have observed that AI and other Machine Learning technologies hold enormous promise in supporting comprehensive efforts to identify and combat the spread of harmful content. While automated tools are just one element of a multifaceted, multilayered safety strategy at Snap, advances in AI technologies (and adjacent developments in the realm of content provenance and authenticity) are unlocking new capabilities in support of critical harm mitigation efforts.

> **b**. Has the FTC ever consulted with your company to learn how your company deploys AI to better detect and combat fraudulent or deceptive content? Has the DOJ? How about the Federal Elections Commission?

Yes. The FTC has issued an order under 6(b) of the FTC Act to eight social media and video streaming services, including Snap, seeking information on how the services scrutinize and restrict paid commercial advertising that is deceptive or exposes consumers to fraudulent healthcare products, financial scams, counterfeit and fake goods, or other fraud. As part of this inquiry, the FTC asked for information about how the services use algorithmic, machine learning, or other automated systems to detect potentially misleading, deceptive, or fraudulent advertisements submitted for publication on Snapchat.

> **c**. How can Congress empower agencies to use AI positively for the protection of American consumers from fraudulent or deceptive content?

We anticipate that different federal agencies will each have distinct uses for AI that can positively advance their mission and help protect consumers; our team would be eager to work with your office to identify high-value opportunities to support these uses.

**6**. Please provide a description of your company's policy regarding the sale or transfer of the data of American users collected on your platform to a third party, including data brokers.

We do not sell user data. We may share data of our users for legitimate business reasons, for example, to cloud storage providers to store user data, and other service providers to enable the services we offer to our users. We detail our practices in our Privacy Policy.

**7**. Has your company ever sold the data of American users on your platform to the government of a foreign country? If so, please provide a full list of the countries and the categories of data sold.

No.

**8**. Outside of complying with a lawful order, has your company ever transferred the data of American users on your platform to the government of a foreign country? If so, please provide a full list of the countries and the circumstances underlying the basis for such transfer.

No, we do not voluntarily transfer data of American users to the government of a foreign country except in limited circumstances where the information relates to an emergency involving danger of death or serious physical injury, which requires the disclosure, as permitted by the U.S. Stored Communications Act.

**9**. Has your company ever sold the data of American users on your platform to a U.S. government agency? If so, please provide a full list of the agencies and the categories of data sold.

No.

**10**. Outside of complying with a lawful order, has your company ever transferred the data of American users on your platform to a U.S. government agency? If so, please provide a full list of the agencies and categories of data transferred.

No, we do not voluntarily transfer data of American users to U.S. government agencies except in limited circumstances where the information relates to illegal conduct or an emergency involving danger of death or serious physical injury, which requires the disclosure, as permitted by the U.S. Stored Communications Act.

**11**. Does your company have a policy to restrict third party use and/or transfer of data collected from users on your platform? Please be specific, including how you enforce such restrictions and whether such restrictions prohibit the sale or transfer of such data to a government agency, including a foreign government agency.

Yes, we restrict the sharing of data with third parties, as detailed in our Privacy Policy. We enforce the Privacy Policy and data sharing restrictions in our privacy-by-design and legal review process, which includes a prohibition on the sale of user data.

**12**. Between July 4, 2023 and July 14, 2023, was your company contacted by any employee of or contractor for any of the following agencies? Please answer "yes" or "no" for each agency and, if "yes," provide the date(s) of contact and the name(s) of the agency employees or contractors that contacted your company.

**a**. U.S. Department of Health and Human Services (HHS)

No.

**b**. National Institute of Allergy and Infectious Diseases (NIAID)

No.

**c**. Centers for Disease Control and Prevention (CDC)

No.

**d**. U.S. Food and Drug Administration (FDA)

No.

**e**. The National Institutes of Health (NIH)

No.

**f**. U.S. Department of Homeland Security (DHS)

Yes. We regularly respond to valid legal requests from employees of the DHS' investigative agency, Homeland Security Investigations.

**g**. DHS Cybersecurity and Infrastructure Security Agency (CISA)

No.

**h**. U.S. Census Bureau

No.

**i**. Federal Bureau of Investigation (FBI)

Yes. We regularly respond to valid legal requests from employees of the FBI.

**j**. U.S. Department of Justice (DOJ)

Yes. We regularly respond to valid legal requests from employees of the DOJ.

**k**. The White House Executive Office of the President (EOP)

No.

**l**. U.S. Department of State

No.

**13**. Is it your company's policy to prevent children under 13 from using your social media app(s) or creating an account?

Yes. When registering a Snapchat account, users are required to accept Snap's Terms of Service, acknowledge the Privacy Policy, and provide their date of birth. Users need to be at least 13 to create a Snapchat account, and the registration process is blocked if a user inputs a birthdate that indicates they are under the age of 13.

If we become aware that a Snapchat user is under the age of 13, we will terminate that user's account and delete the user's data. We also implement a safeguard that prevents younger Snapchat users with existing accounts from updating their birthday to an age of 18 or above. Specifically, if a Snapchat user between the age of 13 to 17 attempts to update their year of birth to reach an age over 18, we will prevent the change.

**14**. In your view, would it be appropriate for school-aged children to spend time on or access your company's social media app(s) during class?

Yes, if it is to communicate with their parents or caregivers regarding an urgent matter.

**15**. As a parent, would you be concerned if your child were able to access your company's social media app(s) during class via a school network or device?

No.

**16**. In your view, should elementary and secondary schools block students' access to your company's social media app(s) on school networks and devices?

No. I am concerned this would unreasonably restrict teen students' ability to communicate with their family and friends.

**17**. Do you think that school buses equipped with Wi-Fi should allow children to access your company's social media app(s) via a school bus Wi-Fi network during their rides to and from school?

Yes. Snapchat is an important communications service for parents and their teens, and using Snapchat before or after school or during a bus ride does not interfere with the classroom environment.

**18**. As a parent, do you think it is important to supervise your children's internet access?

Yes.

**19**. As a parent, would you be concerned if your child's school allowed your child to access the internet on an unsupervised basis, such as on your child's bus ride to and from school via the school bus Wi-Fi?

No. Our family utilizes parental controls that exist on the device level that manages the kind of access and content our child is permitted to view whether using Wi-Fi or cellular data.

**20**. Do you think Congress should require schools, as a condition of receiving broadband subsidies through the Federal Communications Commission's E- Rate program (which funds broadband for elementary and secondary schools), to block students' access to your company's social media app(s) from school-run networks?

No. We believe this decision is better left to parents and schools.

**21**. Do you support the bipartisan Eyes on the Board Act of 2023, S. 3074?

Snap has not taken a formal position on this piece of legislation.

**22**. Have you, your company, or any foundation associated with you or your company, donated or contributed funding, equipment, or services to any of the following organizations in the last ten years (CY 2013 to CY 2023)?

**a**. Education and Libraries Networks Coalition (EdLiNC)
**b**. Open Technology Institute
**c**. Consortium for School Networking (COSN)
**d**. Funds For Learning
**e**. State Educational Technology Directors Association (SETDA)
**f**. Schools, Health, and Libraries Broadband Coalition (SHLB)
**g**. State E-Rate Coordinators' Alliance (SECA)
**h**. EducationSuperHighway
**i**. All4Ed
**j**. Public Knowledge
**k**. Fight for the Future
**l**. Free Press

**m**. Electronic Frontier Foundation
**n**. Benton Foundation or Benton Institute for Broadband & Society
**o**. Electronic Privacy Information Center

No, we have no record of any donations made to these organizations.

**23**. For each such donation or contribution described in the prior question, please detail (1) the type of donation or contribution, such as financial donation, goods or equipment, services, etc.; (2) who made the donation or contribution; (3) the recipient organization; (4) the year the donation or contribution was made; and (5) the total value of that donation or contribution.

N/A