AMBIKA KUMAR (*pro hac vice*)
ambikakumar@dwt.com
DAVIS WRIGHT TREMAINE LLP
920 Fifth Avenue, Suite 3300
Seattle, Washington 98104
Telephone: (206) 757-8030

ADAM S. SIEFF (CA Bar No. 302030)
adamsieff@dwt.com
DAVIS WRIGHT TREMAINE LLP
865 South Figueroa Street, 24th Floor
Los Angeles, California 90017-2566
Telephone: (213) 633-6800

DAVID M. GOSSETT (*pro hac vice*)
davidgossett@dwt.com
MEENAKSHI KRISHNAN (*pro hac vice*)
meenakshikrishnan@dwt.com
DAVIS WRIGHT TREMAINE LLP
1301 K Street NW, Suite 500 East
Washington, D.C. 20005
Telephone: (202) 973-4200

ROBERT CORN-REVERE (*pro hac vice*)
bob.corn-revere@thefire.org
FOUNDATION FOR INDIVIDUAL RIGHTS AND EXPRESSION
700 Pennsylvania Avenue SE, Suite 340
Washington, D.C. 20003
Telephone: (215) 717-3473

Attorneys for Plaintiff
NETCHOICE, LLC d/b/a NetChoice

IN THE UNITED STATES DISTRICT COURT

THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

NETCHOICE, LLC d/b/a NetChoice,

Plaintiff,

v.

ROB BONTA, ATTORNEY GENERAL OF THE STATE OF CALIFORNIA, in his official capacity,

Defendant.

Case No. 5:22-cv-08861-BLF

DECLARATION OF DAVID GOSSETT IN SUPPORT OF NETCHOICE'S MOTION FOR SECOND PRELIMINARY INJUNCTION

I, David Gossett, declare as follows:

1. I am a partner in the law firm Davis Wright Tremaine LLP, counsel for Plaintiff NetChoice LLC. I make this declaration from personal knowledge.

2. Attached as **Exhibit 1** is a true and correct copy of the website page *Policies and community standards*, U.K. Information Commissioner's Office, https://tinyurl.com/5aahfw9r (last visited Oct. 28, 2024).

3. Attached as **Exhibit 2** is a true and correct copy of the website page *Detrimental use of data*, U.K. Information Commissioner's Office, https://tinyurl.com/ysvctbe7 (last visited Oct. 28, 2024).

4. Attached as **Exhibit 3** is a true and correct copy of the website page *Nudge techniques*, U.K. Information Commissioner's Office, https://tinyurl.com/yurvjvft (last visited Oct. 28, 2024).

5. Attached as **Exhibit 4** is a true and correct copy of *Profiling*, U.K. Information Commissioner's Office, https://tinyurl.com/ywt97y7z (last visited Oct. 31, 2024).

6. Attached as **Exhibit 5** is a true and correct copy of Bobby Allyn, *Snapchat Ends "Speed Filter" That Critics Say Encouraged Reckless Driving*, NPR (June 17, 2021).

7. Attached as **Exhibit 6** is a true and correct copy of the website page *Adult Nudity and Sexual Activity*, Meta, https://tinyurl.com/2pbu5ktx (last visited Oct. 28, 2024).

8. Attached as **Exhibit 7** is a true and correct copy of the website page *Bullying and Harassment*, Meta, https://tinyurl.com/4t6pn32s (last visited Oct. 28, 2024).

9. Attached as **Exhibit 8** is a true and correct copy of the website page *Transparency Report July 1, 2023 – December 31, 2023*, Snap, https://tinyurl.com/yc89bsca (updated Apr. 25, 2024).

10. Attached as **Exhibit 9** is a true and correct transcript of the California State Assembly Floor Session held August 30, 2022.

11. Attached as **Exhibit 10** is a true and correct transcript of *Conversation with California Assemblymember Buffy Wicks*, Husch Blackwell (Mar. 7, 2023), https://tinyurl.com/7u2bdxx9.

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

12. Attached as **Exhibit 11** is a true and correct copy of the study *Teens, Social Media and Technology*, Pew Research Center (December 2023).

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed this 1st day of November 2024 in the District of Columbia.

/s/ *David Gossett*
David Gossett

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

CERTIFICATION OF COMPLIANCE

I, Ambika Kumar, hereby certify that pursuant to N.D. Cal. Civil L.R. 5-1, I have obtained authorization from the above signatories to file the above-referenced document and that they have concurred in the filing's content.

Dated: November 1, 2024

Respectfully submitted,

DAVIS WRIGHT TREMAINE LLP

By: /s/ *Ambika Kumar*
Ambika Kumar

Attorneys for Plaintiff
NetChoice, LLC d/b/a NetChoice

DAVIS WRIGHT TREMAINE LLP
865 S. FIGUEROA ST, SUITE 2400
LOS ANGELES, CALIFORNIA 90017-2566
(213) 633-6800
Fax: (213) 633-6899

EXHIBIT 1

Document title:	6. Policies and community standards | ICO
Capture URL:	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/6-policies-and-community-standards/
Page loaded at (UTC):	Mon, 28 Oct 2024 12:32:48 GMT
Capture timestamp (UTC):	Mon, 28 Oct 2024 12:33:17 GMT
Capture tool:	10.52.0
Collection server IP:	54.145.42.72
Browser engine:	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.234 Safari/537.36
Operating system:	Linux (Node 20.17.0)
PDF length:	3
Capture ID:	svSJqShw4aFuqm9gfEbZUh
Display Name:	pauljezick

6. Policies and community standards

Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).

What do you mean by 'upholding your own standards'?

We mean that you need to adhere to your own published terms and conditions and policies.

We also mean that, when you set community rules and conditions of use for users of your service, you need to actively uphold or enforce those rules and conditions.

Why is this important?

Article 5(1) of the GDPR says that personal data shall be:

> "processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')"

When children provide you with their personal data in order to join or access your service they should be able to expect the service to operate in the way that you say it will, and for you to do what you say you are going to do. If this doesn't happen then your collection of their personal data may be unfair and in breach of Article 5(1)(a).

Keeping to your own standards should also benefit you by giving children and their parents confidence that they can trust your online service with their personal data.

How can we make sure that we meet this standard?

To some extent this depends on the content of your published terms and conditions, policies and community standards.

However you should follow the overarching principle that you say what you do and do what you say. You should at least ensure that you do the following:

Only use personal data in accordance with your privacy policy

Article 5(1)(b) of the GDPR sets out the 'purpose limitation' principle, that personal data shall be:

> "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes..."

Articles 13 and 14 of the GDPR require you to tell data subjects what these purposes are. You do this by providing privacy information, which you may include in a privacy notice, policy or statement.

Article 5(1)(a) of the GDPR requires you to process personal data fairly

> "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."

Articles 13 and 14 of the GDPR require you to tell data subjects what these purposes are. You do this by providing privacy information, which you may include in a privacy notice, policy or statement.

Article 5(1)(a) of the GDPR requires you to process personal data fairly and transparently.

The combined result of these provisions is that you need to use your privacy information to tell users what you will do with their personal data and why, and then make sure that you follow this through in practice.

Uphold any user behaviour policies

If you have any published rules which govern the behaviour of users of your service then you need to uphold these rules and put in place the systems that you have said you will. So if you say that you actively monitor user behaviour, or offer real time, automated, or human moderation of 'chat' functions, then you need to do so.

If you only rely on 'back end' processes, such as user reporting, to identify behaviour which breaches your policies then you need to have made that very clear in your policies or community standards. This approach also needs to be reasonable given the risks to children of different ages inherent in your service. If the risks are high then 'light touch' or 'back end only' processes to uphold your standards are unlikely to be sufficient.

If you do not have adequate systems to properly uphold your own user behaviour policies then your original collection and continued use of a child's personal data may be unfair and in breach of the GDPR.

Uphold any content or other policies

If you make commitments to users about the content or other aspects of your online service then you need to have systems to ensure that you meet those commitments.

So if you say that the content of your online service is suitable for children within a certain age range then you need to have systems to ensure that it is. If you say that you do not tolerate bullying, then you need to have adequate mechanisms to swiftly and effectively deal with bullying incidents.

Again, if your systems aren't adequate or you don't keep to your promises then your original collection and continued use of the child's personal data may be unfair and in breach of the GDPR.

If you have different policies depending on the age of your users then you need to take account of the age of the child when upholding your policies.

← Previous Next →

EXHIBIT 2

Document title:	5. Detrimental use of data | ICO
Capture URL:	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/5-detrimental-use-of-data/
Page loaded at (UTC):	Mon, 28 Oct 2024 12:32:48 GMT
Capture timestamp (UTC):	Mon, 28 Oct 2024 12:34:04 GMT
Capture tool:	10.52.0
Collection server IP:	54.145.42.72
Browser engine:	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.234 Safari/537.36
Operating system:	Linux (Node 20.17.0)
PDF length:	5
Capture ID:	hqxTiT3He8JCV4K4vq1Wy9
Display Name:	pauljezick

5. Detrimental use of data

Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions, or Government advice.

What do you mean by 'the detrimental use of data'?

We mean any use of data that is obviously detrimental to children's physical or mental health and wellbeing or that goes against industry codes of practice, other regulatory provisions or Government advice on the welfare of children.

Why is this important?

Article 5(1)(a) of the GDPR says that personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject, and Recital 38 that children merit specific protection with regard to the use of their personal data.

Recital 2 to the GDPR states (emphasis added):

> "The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. **This Regulation is intended to contribute to … the well-being of natural persons.**"

Recital 75 to the GDPR says that:

> "The risk to the rights and freedoms of natural persons, or varying likelihood and severity may result from personal data processing which could lead to physical, material or non-material damage, in particular:....where personal data of vulnerable natural persons, in particular children, are processed...."

This means that you should not process children's personal data in ways that are obviously, or have been shown to be, detrimental to their health or wellbeing. To do so would not be fair.

How can we make sure that we meet this standard?

Keep up date with relevant recommendations and advice

As a provider of an online service likely to be accessed by children you should be aware of relevant standards and codes of practice within your industry or sector, and any provisions within them that relate to children. You should also keep up to date with Government advice on the welfare of children in the context of digital or online services. The ICO does not regulate content and is not an expert on matters of children's health and wellbeing. We will however refer to other codes of practice or regulatory advice where relevant to help us assess your conformance to this standard.

As a provider of an online service likely to be accessed by children you should be aware of relevant standards and codes of practice within your industry or sector, and any provisions within them that relate to children. You should also keep up to date with Government advice on the welfare of children in the context of digital or online services. The ICO does not regulate content and is not an expert on matters of children's health and wellbeing. We will however refer to other codes of practice or regulatory advice where relevant to help us assess your conformance to this standard.

Do not process children's personal data in ways that are obviously detrimental or run counter to such advice

You should not process children's personal data in ways that run contrary to those standards, codes or advice and should take account of any age specific advice to tailor your online service to the age of the child. You should take particular care when profiling children, including making inferences based on their personal data, or processing geo-location data.

You should apply a pre-cautionary approach where this has been formally recommended despite evidence being under debate. This means you should not process children's personal data in ways that have been formally identified as requiring further research or evidence to establish whether or not they are detrimental to the health and wellbeing of children.

What codes or advice are likely to be relevant?

Some specific areas where there is relevant guidance, and that are likely to arise in the context of providing your online service are given below.

However, this is not an exhaustive list and you need to identify and consider anything that is relevant to your specific data processing scenario in your DPIA.

Marketing and behavioural advertising

The Committee of Advertising Practice (CAP) publishes guidance about online behavioural advertising which, in addition to providing rules applicable to all advertising, specifically covers advertising to children.

It includes rules which address:

- physical, mental or moral harm to children;
- exploiting children's credulity and applying unfair pressure;
- direct exhortation of children and undermining parental authority; and
- promotions.

It also has rules which govern or prohibit the marketing of certain products, such as high fat, salt and sugar food and drinks and alcohol, to children, and general guidance on transparency of paid-for content and product placement.

Broadcasting

Ofcom has published a code practice for broadcasters which covers the protection of under-18s in the following areas:

- the coverage of sexual and other offences in the UK involving under-18s;
- drugs, smoking, solvents and alcohol;
- violence and dangerous behaviour;
- offensive language;
- sexual material;
- nudity;
- exorcism, the occult and the paranormal; and
- the involvement of people under 18 in programmes.

The press

The Independent Press Standards Organisation (Ipso) has published The Editors' Code of Practice which includes provisions about reporting and children.

Online games

- the involvement of people under 18 in programmes.

The press

The Independent Press Standards Organisation (Ipso) has published The Editors' Code of Practice which includes provisions about reporting and children.

Online games

The Office for Fair Trading (OFT) has published principles for online and app-based games which includes provisions about:

- exploiting children's inexperience, vulnerability and credulity, including by aggressive commercial practices; and
- including direct exhortations to children to buy advertised products or persuade their parents or other adults to buy advertised products for them.

Strategies used to extend user engagement

Strategies used to extend user engagement, sometimes referred to as 'sticky' features can include mechanisms such as reward loops, continuous scrolling, notifications and auto-play features which encourage users to continue playing a game, watching video content or otherwise staying online.

Although there is currently no formal Government position on the effect of these mechanisms on the health and wellbeing of children, the UK Chief Medical Officers have issued a 'commentary on screen-based activities on children and young people'. This identifies a need for further research and in the meantime recommends that technology companies 'recognise a precautionary approach in developing structures and remove addictive capabilities.'

Does this mean we can't use features such as rewards, notifications and 'likes' within our service?

No, not all such features rely on the use of personal data and you may have designed your feature taking into account the needs of children and in a way that makes it easy for them to disengage without feeling pressurised or disadvantaged if they do so. However, it does mean that you need to carefully consider the impact on children if you use their personal data to support such features. You should consider both intended and unintended consequences of the data use as part of your DPIA.

Given the precautionary advice from the Chief Medical Officers, designing in data-driven features which make it difficult for children to disengage with your service is likely to breach the Article 5(1)(a) fairness principle of the GDPR. For example, features which use personal data to exploit human susceptibility to reward, anticipatory and pleasure seeking behaviours, or peer pressure.

You should:

- avoid using personal data in a way that incentivises children to stay engaged, such as offering children personalised in-game advantages (based upon your use of the individual user's personal data) in return for extended play;
- present options to continue playing or otherwise engaging with your service neutrally without suggesting that children will lose out if they don't;
- avoid features which use personal data to automatically extend use instead of requiring children to make an active choice about whether they want to spend their time in this way (data-driven autoplay features); and
- introduce mechanisms such as pause buttons which allow children to take a break at any time without losing their progress in a game, or provide age appropriate content to support conscious choices about taking breaks, such as that provided in the Chief Medical Officers' advice.

Further reading outside the code

Committee on Advertising Practice guidance

The Ofcom Broadcasting Code (with the Cross-Promotion Code and the On Demand Programme Service Rules)

The Editors' Code of Practice

Does this mean we can't use features such as rewards, recommendations and 'likes' within our service?

No, not all such features rely on the use of personal data and you may have designed your feature taking into account the needs of children and in a way that makes it easy for them to disengage without feeling pressurised or disadvantaged if they do so. However, it does mean that you need to carefully consider the impact on children if you use their personal data to support such features. You should consider both intended and unintended consequences of the data use as part of your DPIA.

Given the precautionary advice from the Chief Medical Officers, designing in data-driven features which make it difficult for children to disengage with your service is likely to breach the Article 5(1)(a) fairness principle of the GDPR. For example, features which use personal data to exploit human susceptibility to reward, anticipatory and pleasure seeking behaviours, or peer pressure.

You should:

- avoid using personal data in a way that incentivises children to stay engaged, such as offering children personalised in-game advantages (based upon your use of the individual user's personal data) in return for extended play;
- present options to continue playing or otherwise engaging with your service neutrally without suggesting that children will lose out if they don't;
- avoid features which use personal data to automatically extend use instead of requiring children to make an active choice about whether they want to spend their time in this way (data-driven autoplay features); and
- introduce mechanisms such as pause buttons which allow children to take a break at any time without losing their progress in a game, or provide age appropriate content to support conscious choices about taking breaks, such as that provided in the Chief Medical Officers' advice.

Further reading outside the code

Committee on Advertising Practice guidance

The Ofcom Broadcasting Code (with the Cross-Promotion Code and the On Demand Programme Service Rules)

The Editors' Code of Practice

OFT principles for online and app-based games

UK Chief Medical Officers' commentary on 'screen based activities and children and young people's mental health and psychosocial wellbeing: a systematic map of reviews'

Previous Next

EXHIBIT 3

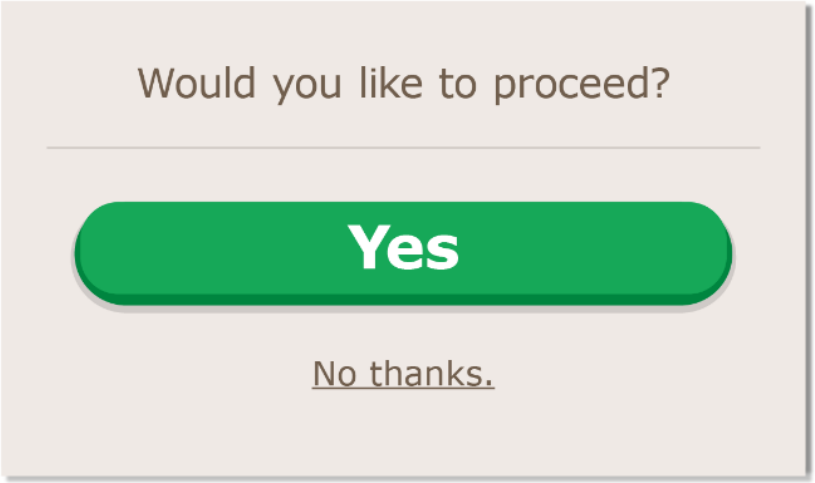
Document title:	13. Nudge techniques | ICO
Capture URL:	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/13-nudge-techniques/
Page loaded at (UTC):	Mon, 28 Oct 2024 12:34:21 GMT
Capture timestamp (UTC):	Mon, 28 Oct 2024 12:34:48 GMT
Capture tool:	10.52.0
Collection server IP:	54.145.42.72
Browser engine:	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.234 Safari/537.36
Operating system:	Linux (Node 20.17.0)
PDF length:	6
Capture ID:	qU8QFbDRV4TTkYJiJo4JcR
Display Name:	pauljezick

13. Nudge techniques

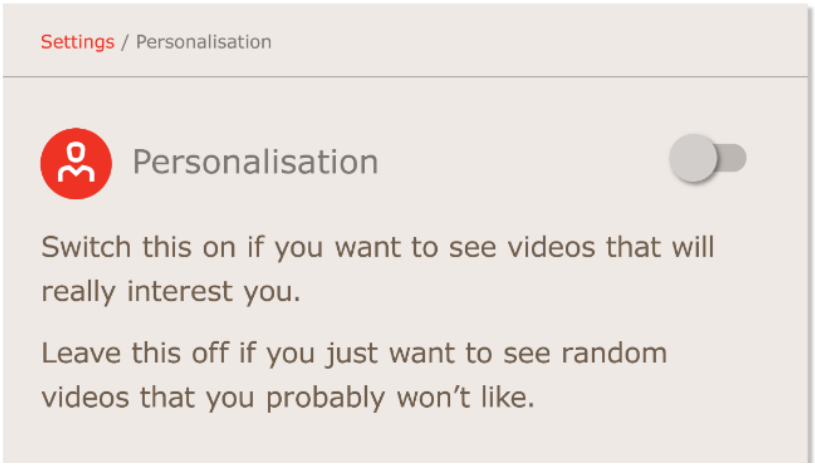
Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or turn off privacy protections.

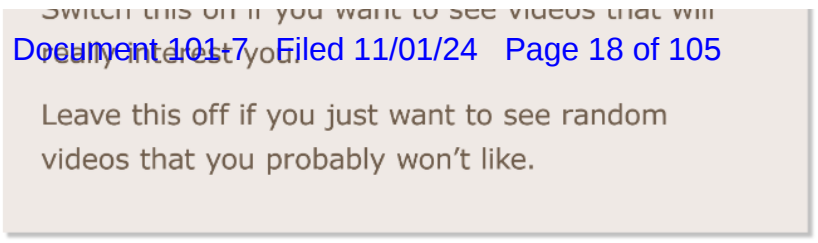
What do you mean by 'nudge techniques'?

Nudge techniques are design features which lead or encourage users to follow the designer's preferred paths in the user's decision making. For example, in the graphic below the large green 'yes' button is presented far more prominently then the small print 'no' option, with the result that the user is 'nudged' towards answering 'yes' rather than 'no' to whatever option is being presented.



In the next example the language used to explain the outcomes of two alternatives is framed more positively for one alternative than for the other, again 'nudging' the user towards the service provider's preferred option.





A further nudge technique involves making one option much less cumbersome or time consuming than the alternative, therefore encouraging many users to just take the easy option. For example providing a low privacy option instantly with just one 'click', and the high privacy alternative via a six click mechanism, or with a delay to accessing the service.

Why is this important?

Article 5(1)(a) of the GDPR says that personal data shall be:

> "processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')"

Recital 38 to the GDPR states that:

> "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data..."

The employment of nudge techniques in the design of online services can be used to encourage users, including children, to provide an online service with more personal data than they would otherwise volunteer. Similarly it can be used to lead users, particularly children, to select less privacy-enhancing choices when personalising their privacy settings.

Using techniques based on the exploitation of human psychological bias in this way goes against the 'fairness' and 'transparency' provisions of the GDPR as well as the child specific considerations set out in Recital 38.

How can we make sure that we meet this standard?

Do not use nudge techniques to lead children to make poor privacy decisions

You should not use nudge techniques to lead or encourage children to activate options that mean they give you more of their personal data, or turn off privacy protections.

You should not exploit unconscious psychological processes to this end (such as associations between certain colours or imagery and positive outcomes, or human affirmation needs).

You should not use nudge techniques that might lead children to lie about their age. For example pre-selecting an older age range for them, or not allowing them the option of selecting their true age range.

Use pro-privacy nudges where appropriate

Taking into account the best interests of the child as a primary consideration, your design should support the developmental needs of the age of your child users.

Younger children, with limited levels understanding and decision making skills need more instruction based interventions, less explanation, unambiguous rules to follow and a greater level of parental support. Nudges towards high privacy options, wellbeing enhancing behaviours and parental controls and involvement should support these needs.

As children get older your focus should gradually move to supporting them in

design should support the developmental needs of the age of your child users.

Younger children, with limited levels understanding and decision making skills need more instruction based interventions, less explanation, unambiguous rules to follow and a greater level of parental support. Nudges towards high privacy options, wellbeing enhancing behaviours and parental controls and involvement should support these needs.

As children get older your focus should gradually move to supporting them in developing conscious decision making skills, providing clear explanations of functionality, risks and consequences. They will benefit from more neutral interventions that require them to think things through. Parental support may still be required but you should present this as an option alongside signposting to other resources.

Consider nudging to promote health and wellbeing

You may also wish to consider nudging children in ways that support their health and wellbeing. For example, nudging them towards supportive resources or providing tools such as pause and save buttons.

If you use personal data to support these features then you still need to make sure your processing is compliant (including having a lawful basis for processing and have providing clear privacy information), but subject to this it is likely that such processing will be fair.

The table below gives some recommendations that you might wish to apply to children of different ages. Although again you are free to develop your own, service specific, user journeys that follow the principle in the headline standard.

You should also consider any additional responsibilities you may have under the applicable equality legislation for England, Scotland, Wales and Northern Ireland.

Age range	Recommendations
0-5 Pre-literate & early literacy	Provide design architecture which is high-privacy by default. If change of default attempted nudge towards maintaining high privacy or towards parental or trusted adult involvement. Avoid explanations – present as rules to protect and help. Consider further interventions such as parental notifications, activation delays or disabling facility to change defaults without parental involvement, depending on the risks inherent in the processing. Nudge towards wellbeing enhancing behaviours (such as taking breaks). Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).
6-9 Core primary school years	Provide design architecture which is high-privacy by default. If change of default attempted nudge towards maintaining high privacy or parental or trusted adult involvement. Provide simple explanations of functionality and inherent risk, but continue to present as rules to protect and help. Consider further interventions such as parental notifications, activation delays or disabling facility to change defaults without parental involvement, depending on the risks inherent in the processing.

	inherent risk, but continue to present as rules to protect and help. Consider further interventions such as parental notifications, activation delays or disabling facility to change defaults without parental involvement, depending on the risks inherent in the processing. Nudge towards wellbeing enhancing behaviours (such as taking breaks). Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).
10-12 Transition years	Provide design architecture which is high-privacy by default. If change of default attempted provide explanations of functionality and inherent risk and suggest parental or trusted adult involvement. Present option in ways that encourage conscious decision making. Consider further interventions such as parental notifications, activation delays or disabling facility to change defaults without parental involvement, depending on the risks. Nudge towards wellbeing enhancing behaviours (such as taking breaks). Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).
13 -15 Early teens	Provide design architecture which is high-privacy by default. Provide explanations of functionality and inherent risk. Present options in ways that encourage conscious decision making. Signpost towards sources of support including parents. Consider further interventions depending on the risks. Suggest wellbeing enhancing behaviours (such as taking breaks). Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).
16-17 Approaching adulthood	Provide design architecture which is high-privacy by default. Provide explanations of functionality and inherent risk. Present options in ways that encourage conscious decision making. Signpost towards sources of support including parents.

	Nudge towards wellbeing enhancing behaviours (such as taking breaks). Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).
13 -15 Early teens	Provide design architecture which is high-privacy by default. Provide explanations of functionality and inherent risk. Present options in ways that encourage conscious decision making. Signpost towards sources of support including parents. Consider further interventions depending on the risks. Suggest wellbeing enhancing behaviours (such as taking breaks). Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).
16-17 Approaching adulthood	Provide design architecture which is high-privacy by default. Provide explanations of functionality and inherent risk. Present options in ways that encourage conscious decision making. Signpost towards sources of support including parents. Suggest wellbeing enhancing behaviours (such as taking breaks). Provide tools to support wellbeing enhancing behaviours (such as mid-level pause and save features).

← Previous

Next →

EXHIBIT 4

12. Profiling

Contents

Switch options which use profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).

What do you mean by 'profiling'?

Profiling is defined in the GDPR:

> "any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour location or movements"

Profiling can be used for a wide range of purposes. It can be used extensively in an online context to suggest or serve content to users, to determine where, when and how frequently that content should be served, to encourage users towards particular behaviours, or to identify users as belonging to particular groups. It can also be used to help establish or estimate the age of a user (as detailed in the standard on age appropriate application), or for child protection, countering terrorism, or the prevention of crime.

Profiles are usually based on a user's past online activity or browsing history. They can be created using directly collected personal data or by drawing inferences (eg preferences or characteristics inferred from associations with other users or past online choices).

Content feeds based on profiling can include advertising content, content provided by other websites, downloads, content generated by other internet users, written, audio or visual content. Profiling may also be used to suggest other users to 'connect with' or 'follow'.

Why is it important?

Profiling is mentioned in Recital 38 to the GDPR as an area in which children merit specific protection with regard to the use of their personal data.

There are also specific rules at Article 22 of the GDPR about decisions (including profiling) which are based solely on the automated processing of personal data, and which have a legal or similarly significant effect on the data subject.

> "22(1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her"

Recital 71 to the GDPR states that such decisions 'should not concern a child'.

The lawfulness, fairness and transparency principle at Article 5(1) is also relevant because this is an area of largely 'invisible processing' in which it is difficult for children to understand how their personal data is being used, and what the consequences of that use might be.

> "5(1) Personal data shall be
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')"

Some profiling may be relatively benign, for example personalisation of a 'walled garden' online environment to incorporate an animal theme in the displayed content. Other profiling, such as content feeds which gradually take the child away from their original area of interest into other less suitable content, raise much more significant concerns.

Should all profiling be controlled by a privacy setting?

It is important to remember that 'off by default' does not mean that profiling is not possible or banned. Following the safeguards and steps set out in this section, which could include effective consent, can enable profiling using children's data to take place, safely and fairly.

There is no point in offering a privacy setting if the profiling is essential to the provision of the core service that the child has requested. This is because if the profiling were turned off there would be no residual service left for the child to use. This concept should be interpreted narrowly, eg that it is completely intrinsic to the service.

However, whenever you can, you should offer children control over whether and how their personal data is used. So most profiling should be subject to a privacy setting. If you can provide a core or residual service without profiling, then you should provide a privacy setting for any additional aspects of your service which rely on profiling.

You should always provide a privacy setting for behavioural advertising which is used to fund a service, but is not part of the core service that the child wishes to access. Although there may be some limited examples of services where behavioural advertising is part of the core service (eg a voucher or 'money off' service), we think these will be exceptional. In most cases the funding model will be distinct from the core service and so should be subject to a privacy setting that is 'off' by default.

There may also be some other limited circumstances in which it won't be appropriate for you to offer a privacy setting over profiling. For example, if you are profiling in order to meet a legal or regulatory requirement (such as a safeguarding or child protection requirement), to prevent child sexual exploitation or abuse online or to age assure so you can properly apply the provisions of this code to child users.

How does this fit with PECR requirements?

Profiling may rely on the use of cookies and similar technologies in order to store or 'remember' the information about a user's past online activity.

A cookie is a small text file that is downloaded onto 'terminal equipment' (eg a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions.

PECR requires that you provide users with clear and comprehensive information about your use of cookies and obtain prior consent for any that are 'non-essential'.

So if you use cookies for the purposes of profiling you need to consider PECR rules for the setting of the cookie, and the GDPR and this code for the underlying processing of personal data (profiling) that the cookie supports or enables.

Profiling and non-essential cookies

If the cookie isn't essential to provide the service that the child wants to access, then the underlying profiling it facilitates normally needs to be subject to a privacy setting. This gives the child control over whether their personal data is used for this purpose.

You need consent for the cookie as well as a GDPR lawful basis for processing for the underlying processing (in practice this may also be consent).

Cookies, profiling, and your core services

If the cookie is essential to the provision of your core service then it is likely that the underlying profiling that the cookie enables is too. In this circumstance providing a privacy setting which allows the child to control whether their personal data is used for this purpose won't be appropriate. You need a lawful basis (other than consent) for the underlying processing (profiling) and won't need consent for the cookie.

Cookies, profiling and your non-core services

Cookies may also be essential for providing your non-core services. However, as these are optional elements of your service you firstly need to provide a privacy setting which gives the child control over whether they wish their personal data to be processed in order to access them.

If the child decides to do so, then you do not need consent for the use of the cookie – as the child is specifically requesting to access part of your service and the cookie is strictly necessary for this purpose.

You do however need a lawful basis for the underlying processing.

Cookies, profiling, and age estimation or age assurance

You may also use cookies for profiling that intends to meet the implied age verification requirements of Article 8 of the GDPR, or to age assure in order to properly apply the standards of this code. For more detail about the Article 8 requirements see Annex C Lawful bases for processing.

In this circumstance, the purpose you use the cookies for is regarded as essential for the service, as you need to do so to provide an age appropriate service and comply with the GDPR. Provided that the cookie in question is solely used for this purpose, and not for any other purpose, then the child does not need to consent to the cookie.

For more information about cookies, and when a cookie is essential and non-essential, see our guidance on Cookies and similar technologies.

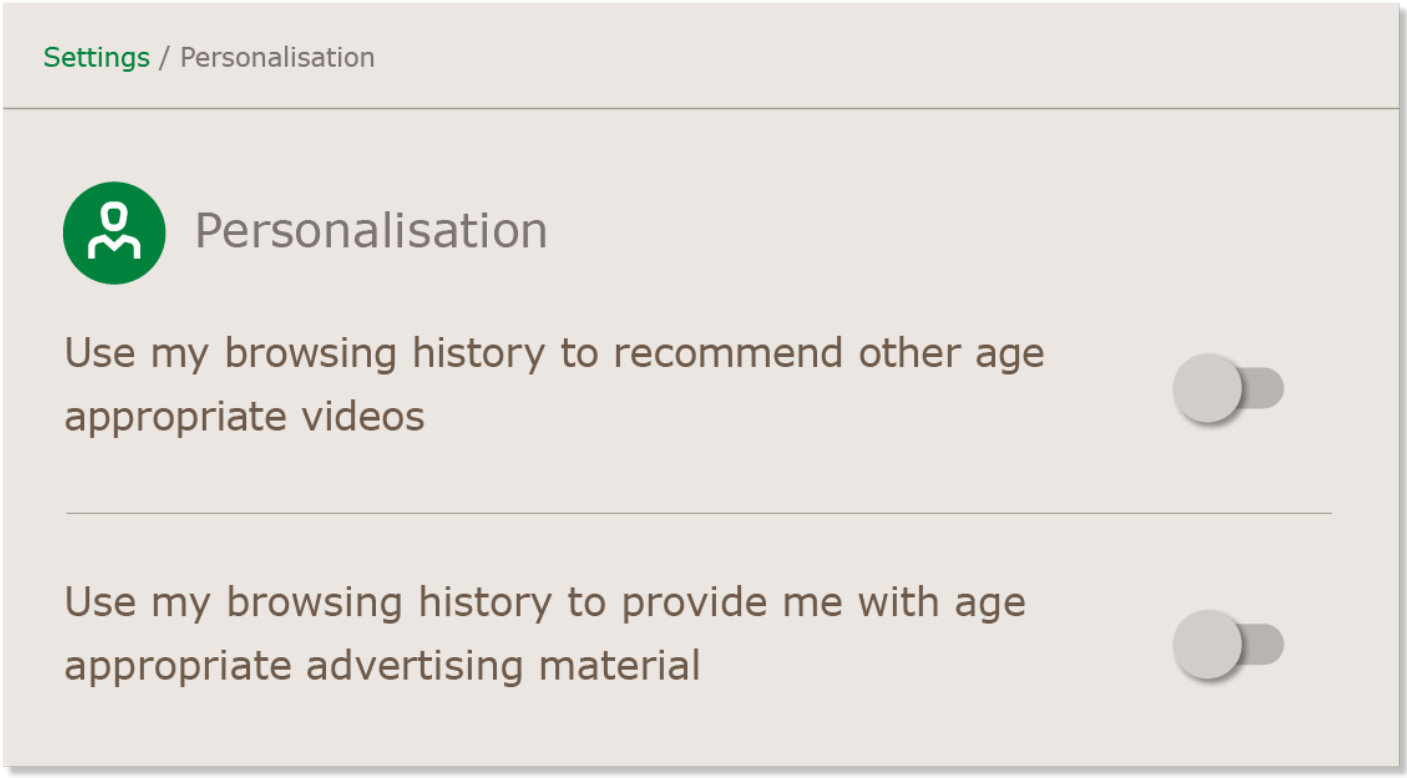
How can we make sure that we meet this standard?

Differentiate between different types of profiling for different purposes

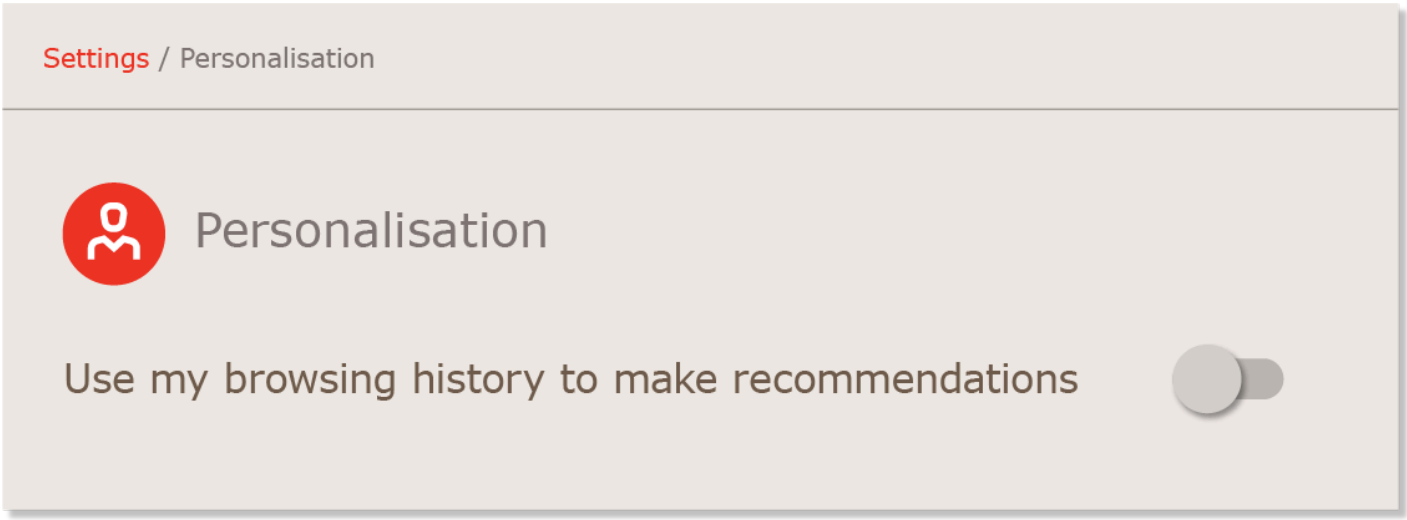
Because profiling can be used to serve a wide range of purposes it is particularly important to be clear about the purposes for which your service uses personal data to profile its users, and to differentiate between them. Catch-all purposes, such as 'providing a personalised service' are not specific enough.

Where it is appropriate to offer privacy settings then you should offer separate settings for each different type of profiling. It is not acceptable to bundle different types of profiling together under one privacy setting, or to bundle in profiling with processing for other purposes.

Acceptable practice:



Unacceptable practice:



Ensure features that rely on profiling are switched off by default (unless there is a compelling reason to do otherwise)

You need to switch any options within your service which rely on profiling off by default, unless you can demonstrate a compelling reason why this should not be the case, taking account of the best interests of the child. You need to assess this in the specific circumstances of your processing.

In practice it is likely to mean that any non-essential features that rely on profiling and that you provide for commercial purposes are subject to a privacy setting which is switched off by default.

In the case of any profiling you do for the purposes of behavioural advertising, which is facilitated by cookies, this approach is supported by the comments of the EDPB. EDPB have indicated that 'legitimate interests' is unlikely to provide a valid lawful basis for processing for this purpose which means that consent is your only viable basis for processing. As valid consent has to be 'opt in', allowing such profiling 'by default' is not an option. You also need to comply with the Article 8 GDPR requirements for parental consent if the child is under the age of 13. For more information about lawful bases for processing and Article 8 requirements see Annex C.

However, you may have a compelling argument that you need to switch profiling options for other purposes on by default.

For example, it may be appropriate for profiling for the purposes of ensuring that a service is accessible to a disabled child (eg identifying that a child has an ongoing need for a subtitled, signed or other supported service) to be switched on by default.

You may be able to demonstrate that profiling for the purposes of informing news content feeds should be allowed by default, in order to recognise the rights of children to access information. Although you still need consent to set the cookies that support the profiling in

accordance with PECR requirements. This is more likely to be the case if you can demonstrate that you conform with existing regulatory codes of practice which govern media content and practices (such as The Editors' Code of Practice) and have editorial control over the content that children will be shown as a result of the profiling. It is unlikely to apply if you do not have such editorial control or adhere to other regulatory controls. See also our FAQs for the news media.

Provide appropriate interventions at the point at which any profiling is activated

At the point any profiling options are turned on, you need to provide age appropriate information about what will happen to the child's personal data and any risks inherent in that processing.

You should also provide age appropriate prompts to seek assistance from an adult and not to activate the profiling if they are uncertain or don't understand.

Depending on your assessment of risk and the age of the child you may wish to make further interventions, which might include further age assurance measures.

If profiling is on ensure that you put appropriate measures in place to safeguard the child (in particular from inappropriate content)

If your online service uses any profiling then you need to take appropriate steps to make sure that this does not result in harm to the child.

In practice this means that if you profile children (using their personal data) in order to suggest content to them, then you need suitable measures in place to make sure that children aren't served content which is detrimental to their physical or mental health or wellbeing, taking into account their age. As covered in the section of this code on DPIAs, testing your algorithms should assist you in assessing the effectiveness of your measures.

Such measures could include contextual tagging, robust reporting procedures, and elements of human moderation. It could also include your own editorial controls over the content you display, including adherence to codes of conduct or other regulatory provisions (such as compliance with The Editors' Code of Practice, or the Ofcom Broadcasting Code). We recognise the importance of the rights of children to access information from the media, and the societal and developmental benefits of children being able to engage in current affairs and the world around them. We would therefore accept that adherence to editorial or broadcasting codes of conduct negate the need for providers of online news to take any additional steps in relation to news content for children. See also our FAQs for the news media.

If you are using children's personal data to automatically recommend content to them based on their past usage/browsing history then you have a responsibility for the recommendations you make. This applies even if the content itself is user generated. In data protection terms, you have a greater responsibility in this situation than if the child

were to pro-actively search out such content themselves. This is because it is your processing of the personal data that serves the content to the child. Data protection law doesn't make you responsible for third party content but it does make you responsible for the content you serve to children who use your service, based on your use of their personal data.

Your general approach should be that if the content you promote or the behaviours your features encourage are obviously detrimental, or are recognised as harmful to the child, in one context (eg marketing rules, film classification, advice from official Government sources such as Chief Medical Officers' advice, PEGI ratings) then you should assume that the same type of content or behaviour is harmful in other contexts as well. Where evidence is inconclusive you should apply the same precautionary principle.

Content or behaviours that may be detrimental to children's health and wellbeing (taking into account their age) include:

- advertising or marketing content that is contrary to CAP guidelines on marketing to children;
- film or on-demand television content that is classified as unsuitable for the age group concerned;
- music content that is labelled as parental advisory or explicit;
- pornography or other adult or violent content;
- user generated content (content that is posted by other internet users) that is obviously detrimental to children's wellbeing or is formally recognised as such (eg pro-suicide, pro-self harm, pro-anorexia content. Content depicting or advocating risky or dangerous behaviour by children); and
- strategies used to extend user engagement, such as timed notifications that respond to inactivity.

Ultimately, if you believe that it is not feasible for you to put suitable measures in place, then you are not be able to profile children for the purposes of recommending online content. In this circumstance you need to make sure that children cannot change any privacy settings which allow this type of profiling.

Similarly, if you cannot put suitable measures in place to safeguard children from harms arising from profiling for other purposes (such as profiling to promote certain behaviours), you should not profile children for these purposes either.

How does this fit with other rules on restricting access to content for children?

You may need to take account of other rules on restricting access to content in order to ensure that you don't use children's personal data in ways that have been shown to be detrimental to their wellbeing (for more detail see the standard on detrimental use of data).

The CAP code requires that when advertising is targeted through the use of personal data, advertisers must show that they have taken reasonable steps to reduce the likelihood of those who are, or are likely to be, in a protected age category being exposed to age-restricted marketing content.

The Ofcom On Demand Programme Service Rules require providers of 'on demand' content to only make certain content ('specially restricted material') available, if it can do so in a way that ensures that those under the age of 18 will not normally be able to see or hear it.

The Audiovisual Media Services Directive 2018 (AVMSD) (if implemented in the UK) will require 'video sharing platform services' to use proportionate measures in relation to how they organise the content they share, to protect minors from content which might impair their physical, mental or moral development.

We consider that it is consistent with these provisions to only allow children's personal data to be used to determine content feeds if you can put suitable measures in place to guard against them being served content that is detrimental to their health and wellbeing

The AVMSD also requires that you should not use personal data collected or generated for the purposes of protecting minors from content which might impair their physical, mental or moral development for commercial purposes such as direct marketing, profiling and behaviourally targeted advertising.

We consider that this requirement is consistent with the purpose limitation principle of the GDPR and with our guidance in the sections of this code on age appropriate application - What if we need to collect personal data in order to establish age? It doesn't mean that services within the scope of the AVMSD can't ever process personal data for commercial purposes. It just means that you can't use personal data collected for one purpose for another. If such services wish to profile children for the purpose of behavioural advertising you will need the child's (or parent's) consent. For more information on consent see Annex C Lawful bases for processing.

We will work with other regulators as necessary where issues of regulatory consistency arise.

Further reading outside this code

The Editors' Code of Practice

The Ofcom Broadcasting Code (with the Cross-promotion Code and the on Demand Programme Service Rules)

Directive (EU) 2018/1808 amending Directive 2010/13/EU (Audiovisual Media Services Directive) and the UK government's Audiovisual Media Services Consultation Document

Age Appropriate Design Code FAQs for the news media

EXHIBIT 5

TECHNOLOGY

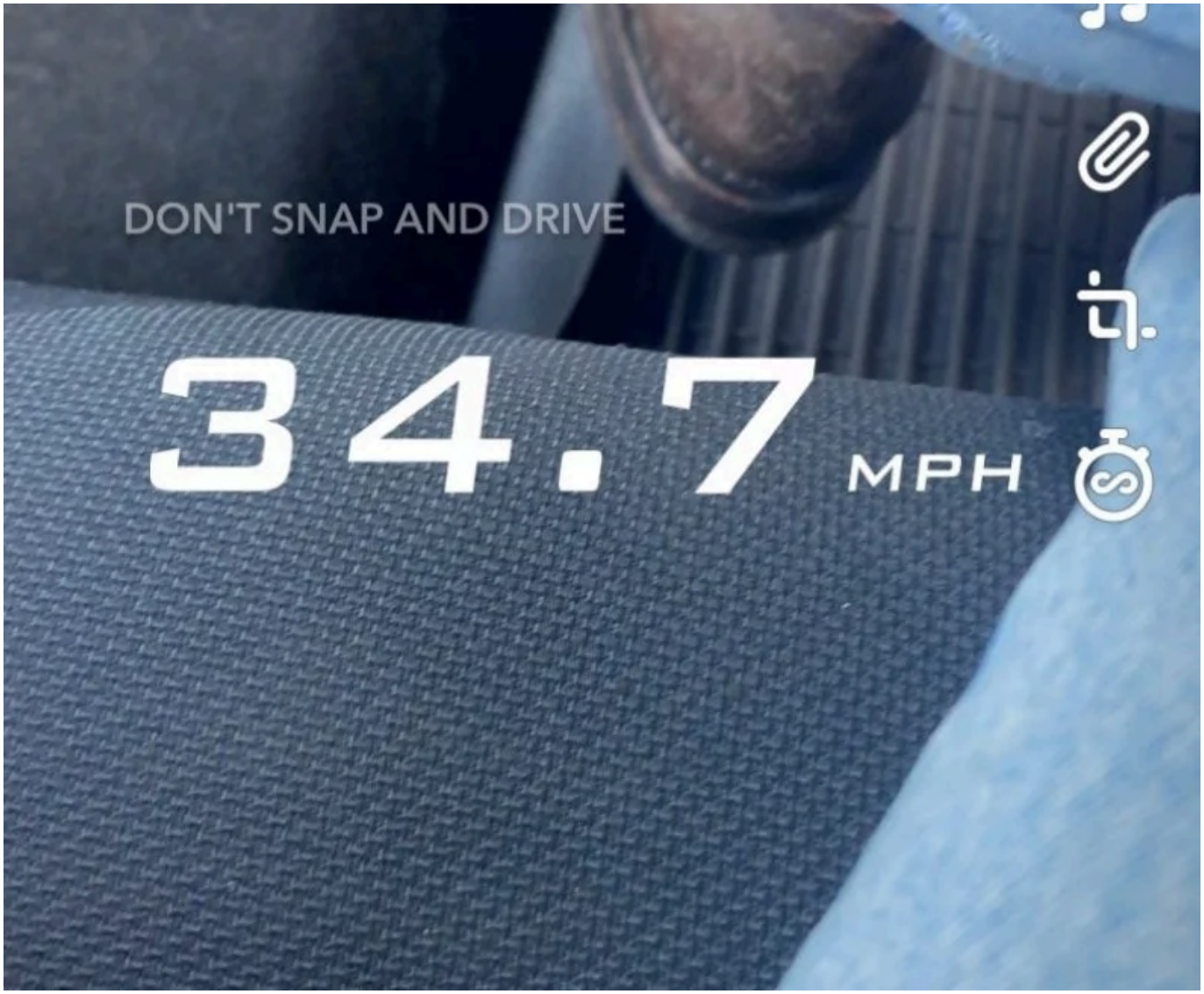
Snapchat Ends 'Speed Filter' That Critics Say Encouraged Reckless Driving

JUNE 17, 2021 · 11:58 AM ET

HEARD ON ALL THINGS CONSIDERED

Bobby Allyn

3-Minute Listen



An iPhone screengrab of Snapchat's speed filter, which allows users to record and share how fast they are moving. Snap told NPR that it is eliminating the tool.

Bobby Allyn/NPR

The maker of the Snapchat app is eliminating a feature known as the "speed filter" that lets users capture how fast they are moving and share it with friends, NPR has learned.

The move is a dramatic reversal for Snap, Inc., which introduced the feature in 2013.

Since then, Snap has defended the feature in the face of warnings from safety advocates who have argued that it encourages reckless driving. The company has also faced lawsuits from the families of those who have been injured or killed in car crashes where drivers were moving at excessive speeds, allegedly to score bragging rights on the app.

Critics of the speed filter welcomed the news, while also questioning the delay.

"Lives will be saved. Crashes will be prevented, but the lawyer in me says, 'My God, why did it take so long?' " said Joel Feldman, the co-founder of the nonprofit End Distracted Driving, one of the groups that urged Snapchat to remove the speed filter.

What exactly led Snap to scrap the feature now is unclear. Over several weeks, NPR asked Snap a series of questions about why it had stood by the speed filter for so long. A company spokeswoman told NPR, "Nothing is more important than the safety of our Snapchat community."

A month later, the same spokeswoman confirmed the speed filter would soon be gone.

The feature "is barely used by Snapchatters," she said on Thursday. "And in light of that, we are removing it altogether."

She said the company started removing the feature this week, but it may be a couple weeks before it disappears from the app for all of its 500 million monthly active users.

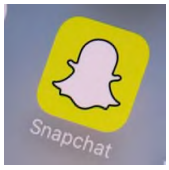
Lawyer Michael Neff, who has represented the families of those involved in car crashes linked to the filter, said the change does not undo the pain of his clients.

"While this will no doubt serve the safety of the motoring public moving forward, it does not remedy Snapchat's choice to create and distribute the speed filter in the past," Neff said. "We look forward to our day in court and pursuing justice for those who suffered unnecessary losses."

'Speed filter' involved in several deadly car crashes

The feature has been connected to a number of deadly or near-fatal car crashes, often with teenagers behind the wheel.

A 2015 collision involving the speed filter left a driver in Georgia with permanent brain damage. That same year, the feature was tied to the death of three young women in a Philadelphia car accident. In 2016, five people in Florida died in a high-speed collision that reportedly involved the speed filter. In 2017, three young men in Wisconsin clocked a speed of 123 miles per hour on the feature before they crashed into a tree and died.



TECHNOLOGY

Snapchat Can Be Sued Over Role In Fatal Car Crash, Court Rules

In response, Snap made a number of changes. It moved the speed feature from a "filter" to a "sticker" in Snapchat, lowering its prominence. It also added a "Don't Snap and drive" warning that would appear every time someone used the feature.

The company also quietly capped the top speed for which a post could be shared for "driving speeds" at 35 mph. When NPR inquired about this in May, the Snap spokeswoman confirmed that the limitation had been imposed. Yet the company kept the filter available for use.

And the legal battles continue. Naveen Ramachandrappa, a California lawyer who sued Snap over the speed filter, wrote in a lawsuit that some teenage users of Snap believed they would be rewarded with digital prizes and trophies for recording a speed in excess of 100 miles per hour.

"Or at the very least, they want to find out if they will be so rewarded and so they drive at excessive speeds to see what will happen," he wrote.

A federal appeals court in May ruled that the family of the young men who died in the Wisconsin crash should be able to sue Snap for being negligent in designing a product that led to foreseeable harm. Snap this week asked the trial court to toss the case out, arguing the speed filter did not cause the car accident.

Of the some 5 billion "snaps" users make every day, the speed feature barely registers in terms of popularity, which is why Snap officials say it is dropping the tool.

Irina Raicu, the director of the Internet Ethics Program at Santa Clara University, said that increasingly, tech companies are doing risk assessments of new products

and features to try to get ahead of possible abuses.

"If you have a new tool or feature: What does it allow? What does it invite? And what does it incentivize? There are degrees of responsibility based on those three things," she said. "This Snapchat filter seems like maybe it was missing some of those conversations initially."

"Sometimes," Raicu added, "one of the most thoughtful ways to deploy a product is to never deploy it at all."

snapchat speed filter

More Stories From NPR

EXHIBIT 6

Document title:	Community Standards Enforcement | Transparency Center
Capture URL:	https://transparency.meta.com/reports/community-standards-enforcement/adult-nudity-and-sexual-activity/facebook/
Page loaded at (UTC):	Mon, 28 Oct 2024 12:29:10 GMT
Capture timestamp (UTC):	Mon, 28 Oct 2024 12:30:45 GMT
Capture tool:	10.52.0
Collection server IP:	54.145.42.72
Browser engine:	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.234 Safari/537.36
Operating system:	Linux (Node 20.17.0)
PDF length:	6
Capture ID:	widWsQ388KA9hbMd3hoadP
Display Name:	pauljezick

Adult Nudity and Sexual Activity

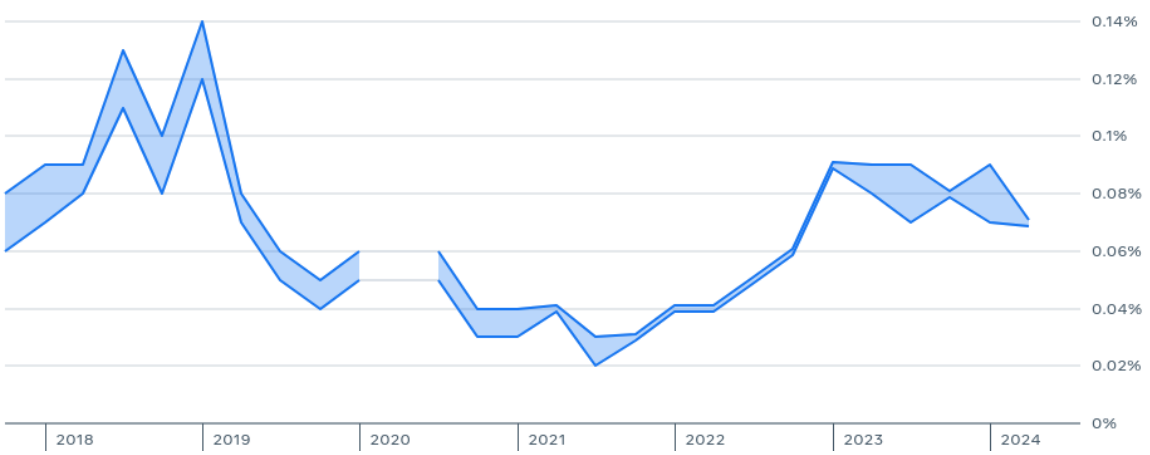
We restrict the display of adult nudity and sexual activity on Facebook and Instagram. We make some exceptions when it is clear the content is being shared in the context of a protest, for educational or medical reasons or a similar reason. On the other hand, we default to removing sexual imagery to prevent non-consensual or underage content from being shared.

This report does not include metrics related to our separate policy on the promotion of sexual assault, violence or exploitation.

Read the policy details

PREVALENCE

How prevalent were adult nudity and sexual activity violations?



Facebook

Overview

Adult Nudity and Sexual Activity

Bullying and Harassment

Child Endangerment: Nudity and Physical Abuse and Sexual Exploitation

Dangerous Organizations: Terrorism and Organized Hate

Fake Accounts

Hate Speech

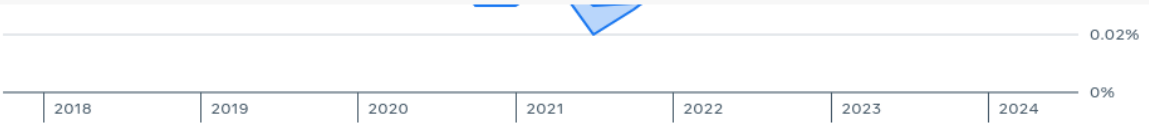
Restricted Goods and Services

Spam

Suicide and Self-Injury

Violence and Incitement

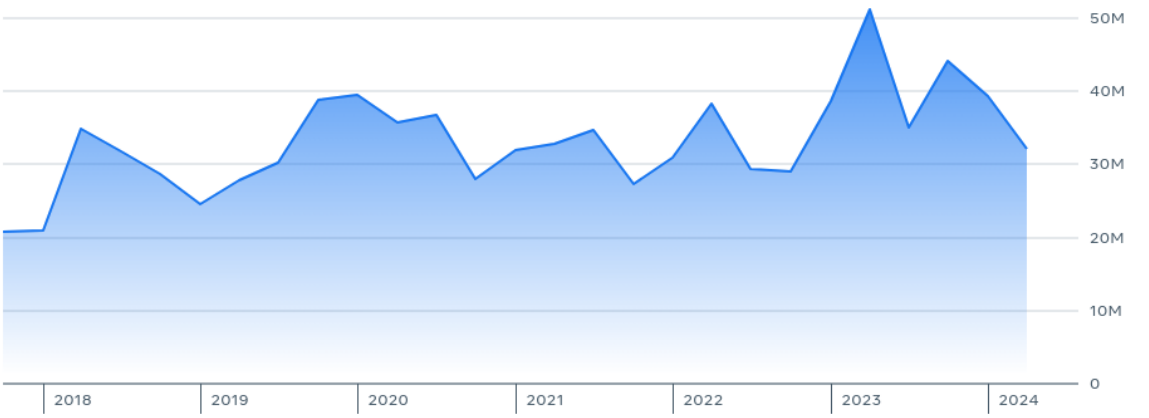
Violent and Graphic Content



How we calculate it ⓘ Read about this data ⊕

CONTENT ACTIONED

How much adult nudity and sexual activity content did we take action on?



How we calculate it ⓘ Read about this data ⊕

PROACTIVE RATE

Of the violating content we actioned for adult nudity and sexual activity, how much did we find and action before people reported it?

Facebook

Overview

Adult Nudity and Sexual Activity

Bullying and Harassment

Child Endangerment: Nudity and Physical Abuse and Sexual Exploitation

Dangerous Organizations: Terrorism and Organized Hate

Fake Accounts

Hate Speech

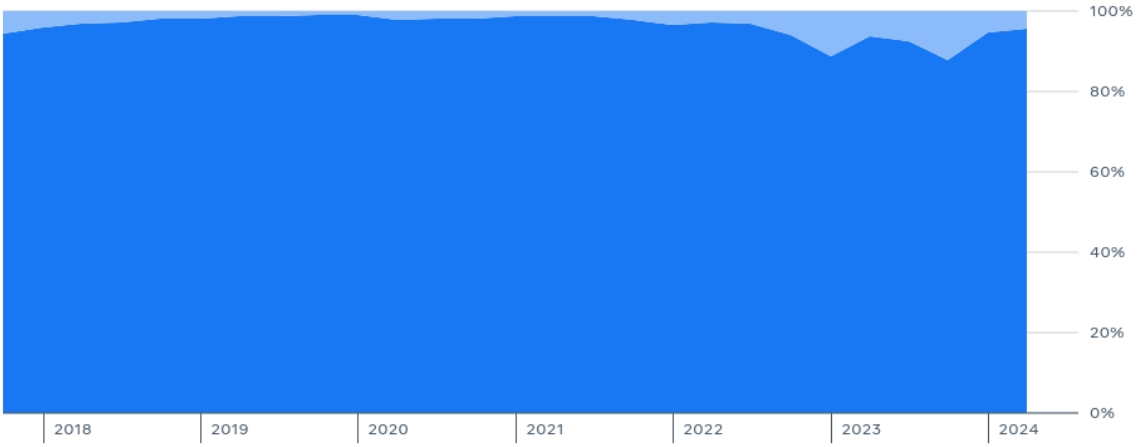
Restricted Goods and Services

Spam

Suicide and Self-Injury

Violence and Incitement

Violent and Graphic Content



How we calculate it **Read about this data**

Correcting mistakes

People can appeal our decisions, unless there are extreme safety concerns. We restore content we incorrectly removed or when circumstances change. Restores can happen from appeals or when we identify issues ourselves.

APPEALED CONTENT

How much of the content we actioned for adult nudity and sexual activity did people appeal?

Facebook

Overview

Adult Nudity and Sexual Activity

Bullying and Harassment

Child Endangerment: Nudity and Physical Abuse and Sexual Exploitation

Dangerous Organizations: Terrorism and Organized Hate

Fake Accounts

Hate Speech

Restricted Goods and Services

Spam

Suicide and Self-Injury

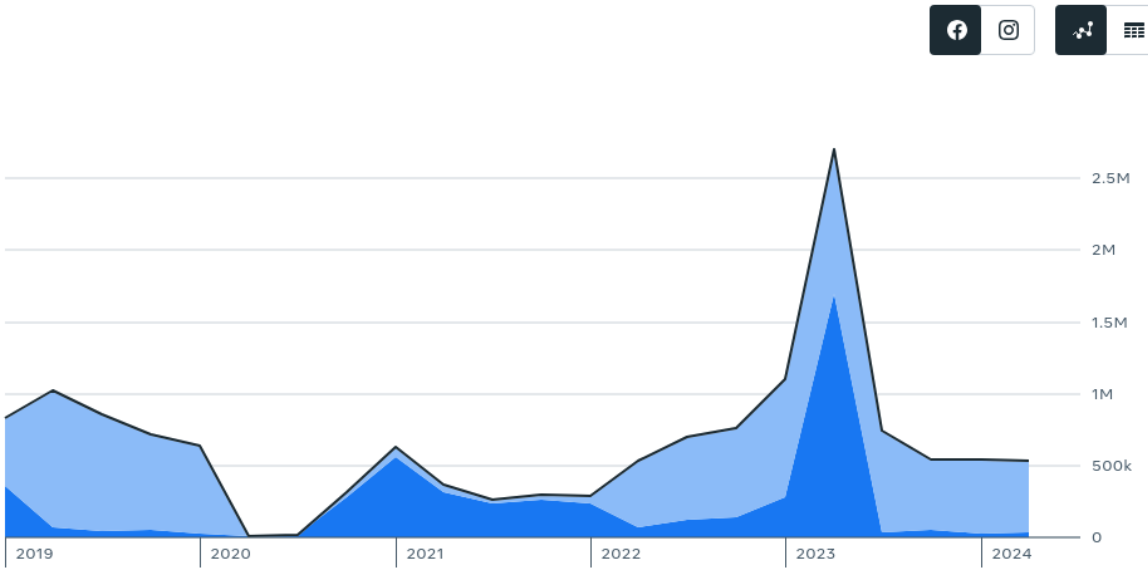
Violence and Incitement

Violent and Graphic Content

How we calculate it ⓘ Read about this data ⓘ

RESTORED CONTENT

How much actioned content for adult nudity and sexual activity was later restored?



How we calculate it ⓘ Read about this data ⓘ

PREVIOUS
Overview

NEXT
Bullying and Harassment

PREVIOUS
Overview

NEXT
Bullying and Harassment

Meta

Transparency Center

EXHIBIT 7

Document title:	Community Standards Enforcement | Transparency Center
Capture URL:	https://transparency.meta.com/reports/community-standards-enforcement/bullying-and-harassment/facebook/
Page loaded at (UTC):	Mon, 28 Oct 2024 12:31:02 GMT
Capture timestamp (UTC):	Mon, 28 Oct 2024 12:31:31 GMT
Capture tool:	10.52.0
Collection server IP:	54.145.42.72
Browser engine:	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.234 Safari/537.36
Operating system:	Linux (Node 20.17.0)
PDF length:	6
Capture ID:	wXSLHRY5V96orSgZgzs9Jy
Display Name:	pauljezick

Bullying and Harassment

We do not tolerate bullying and harassment on Facebook and Instagram. Because we recognize bullying can be especially harmful for minors, our policies provide heightened protections for them. We want to allow for open and vital discussion of people who are in the news or who have a large public audience, so we do permit more open or critical discourse towards public figures than private individuals.

Because bullying and harassment is highly personal by nature, using technology to proactively detect these behaviors can be more challenging than other types of violations. That's why we also rely on people to report this behavior to us so we can identify and remove it. When measuring prevalence in this area, the metric captures only bullying and harassment where a deeper understanding of context or meaning is not necessary to determine if it violates our policy. We continue to invest in our proactive detection technology to ensure we are tackling the problem and protecting our community.

Read the policy details

PREVALENCE

How prevalent were bullying and harassment violations?

Facebook

Overview

Adult Nudity and Sexual Activity

Bullying and Harassment

Child Endangerment: Nudity and Physical Abuse and Sexual Exploitation

Dangerous Organizations: Terrorism and Organized Hate

Fake Accounts

Hate Speech

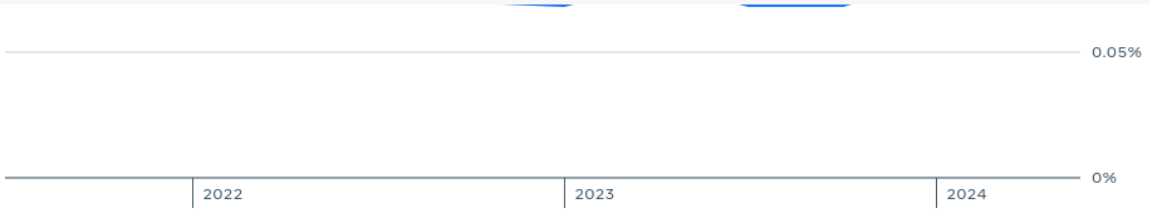
Restricted Goods and Services

Spam

Suicide and Self-Injury

Violence and Incitement

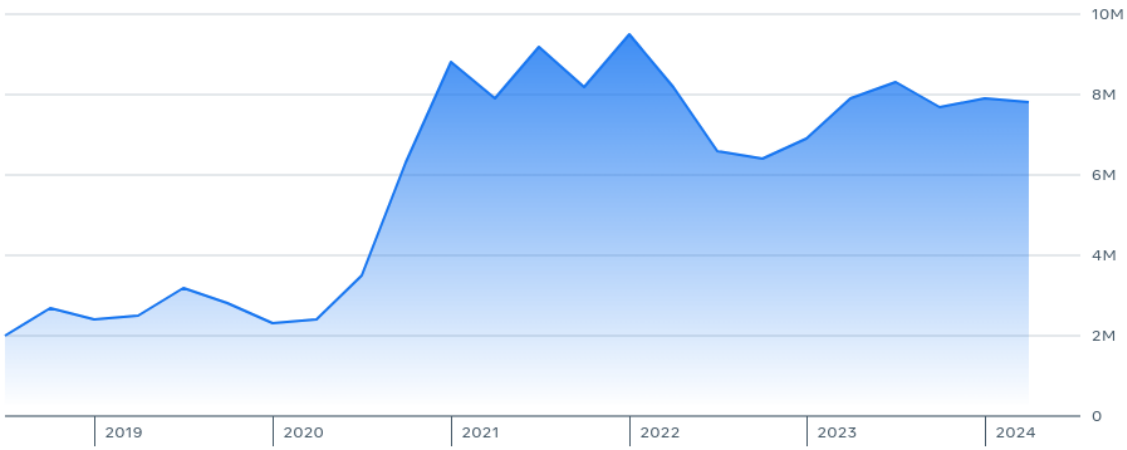
Violent and Graphic Content



How we calculate it Read about this data

CONTENT ACTIONED

How much bullying and harassment content did we take action on?



How we calculate it Read about this data

PROACTIVE RATE

Of the violating content we actioned for bullying and harassment, how much did we find and action before people reported it?

Facebook

Overview

Adult Nudity and Sexual Activity

Bullying and Harassment

Child Endangerment: Nudity and Physical Abuse and Sexual Exploitation

Dangerous Organizations: Terrorism and Organized Hate

Fake Accounts

Hate Speech

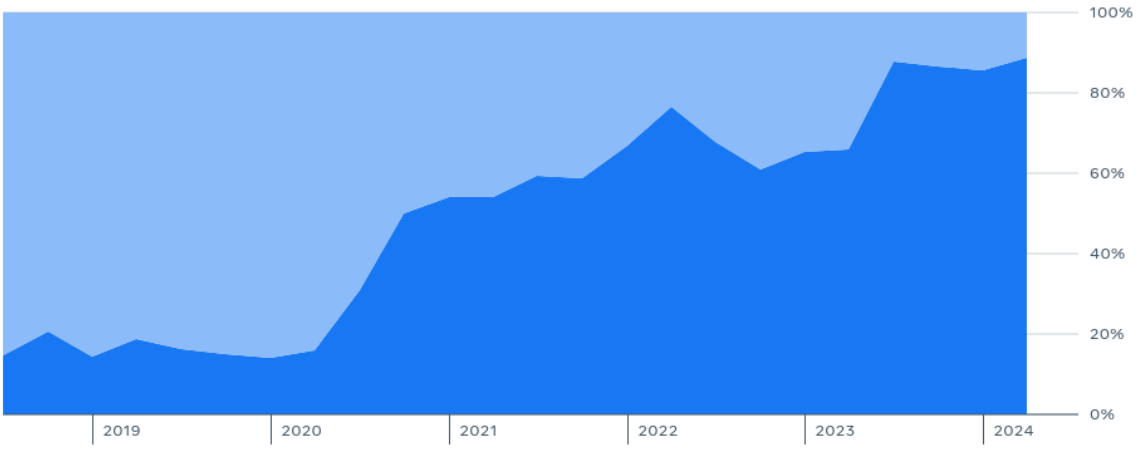
Restricted Goods and Services

Spam

Suicide and Self-Injury

Violence and Incitement

Violent and Graphic Content



How we calculate it **Read about this data**

Correcting mistakes

People can appeal our decisions, unless there are extreme safety concerns. We restore content we incorrectly removed or when circumstances change. Restores can happen from appeals or when we identify issues ourselves.

APPEALED CONTENT

How much of the content we actioned for bullying and harassment did people appeal?

Facebook

Overview

Adult Nudity and Sexual Activity

Bullying and Harassment

Child Endangerment: Nudity and Physical Abuse and Sexual Exploitation

Dangerous Organizations: Terrorism and Organized Hate

Fake Accounts

Hate Speech

Restricted Goods and Services

Spam

Suicide and Self-Injury

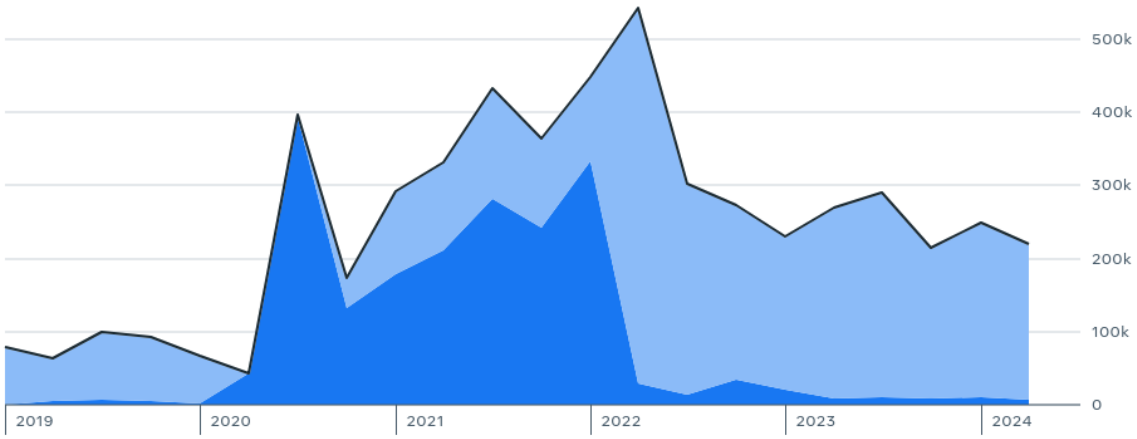
Violence and Incitement

Violent and Graphic Content

How we calculate it Read about this data

RESTORED CONTENT

How much actioned content for bullying and harassment was later restored?



How we calculate it Read about this data

PREVIOUS
Adult Nudity and Sexual Activity

NEXT
Child Endangerment: Nudity and Physical Abuse and Sexual

PREVIOUS
Adult Nudity and Sexual Activity

NEXT
Child Endangerment: Nudity and Physical Abuse and Sexual Exploitation

Meta

Transparency Center

EXHIBIT 8

Document title:	Snapchat Transparency Report | Snapchat Transparency
Capture URL:	https://values.snap.com/privacy/transparency?lang=en-US#:~:text=Overview%20of%20Content%20and%20Account%20Violations&text=During%20the%20reporting%20period%2C%20we,found%20to%20violate%20our%20policies.
Page loaded at (UTC):	Mon, 28 Oct 2024 12:31:49 GMT
Capture timestamp (UTC):	Mon, 28 Oct 2024 12:32:18 GMT
Capture tool:	10.52.0
Collection server IP:	54.145.42.72
Browser engine:	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.234 Safari/537.36
Operating system:	Linux (Node 20.17.0)
PDF length:	8
Capture ID:	6Sc57U9DLW6JMzfETDmDbN
Display Name:	pauljezick

Transparency Report

July 1, 2023 – December 31, 2023

Released:

April 25, 2024

Updated:

April 25, 2024

To further provide insight into Snap's safety efforts and the nature and volume of content reported on our platform, we publish this transparency report twice a year. We are committed to continuing to make these reports more comprehensive and informative to the safety and well-being of our community, and the many stakeholders who care deeply about our content moderation and law enforcement practices.

This Transparency Report covers the second half of 2023 (July 1 - December 31). As with our previous reports, we share data about the global number of in-app content and account-level reports we received and enforced across specific categories of policy violations; how we responded to requests from law enforcement and governments; and our enforcement actions broken down by country.

As part of our ongoing commitment to continually improve our transparency reports, we are introducing a few new elements with this release.

First, we have expanded our main table to include reports and enforcement against content and accounts tied to both Terrorism & Violent Extremism and Child Sexual Exploitation & Abuse (CSEA). In previous reports, we had highlighted account deletions made in response to those violations in separate sections. We will continue to outline our proactive and reactive efforts against CSEA, as well as our reports to NCMEC, in a separate section.

Second, we have provided expanded information on appeals, outlining total appeals and reinstatements by Community Guidelines enforcements.

Finally, we have expanded our **European Union** section, providing increased insight into Snap's EU activities. Specifically, we are publishing our most recent DSA Transparency Report and additional metrics regarding our CSEA media scanning.

For more information about our policies for combating online harms, and plans to continue evolving our reporting practices, please read our recent **Safety & Impact blog** about this Transparency Report. To find additional safety and privacy resources on Snapchat, see our ***About Transparency Reporting*** tab at the bottom of the page.

Please note that the most up-to-date version of this Transparency Report can be found in the en-US locale.

Overview of Content and Account Violations

From July 1 - December 31, 2023, Snap enforced against 5,376,714 pieces of content globally that were reported to us and violated our Community Guidelines.

During the reporting period, we saw a Violative View Rate (VVR) of 0.01 percent, which means that out of every 10,000 Snap and Story views on Snapchat, 1 contained content found to violate our policies. The median turnaround time to enforce reported content was ~10 minutes.

Total Content & Account Reports	Total Content Enforced	Total Unique Accounts Enforced
19,041,510	5,376,714	3,315,759

Transparency
- Transparency Report
- About
- Glossary
- Previous Reports
- European Union
- Ads Gallery
- Australia
- California
- India
- Researchers

19,041,510	5,376,714	3,315,759

Reason	Content & Account Reports	Content Enforced	% of the Total Content Enforced by Snap	Unique Accounts Enforced	Turnaround Time (in median minutes)
Sexual Content	4,271,116	2,266,213	42.1%	1,321,205	7
Child Sexual Exploitation	847,430	239,820	4.5%	206,904	52
Harassment and Bullying	8,524,054	1,193,695	22.2%	934,994	7
Threats & Violence	836,125	114,315	2.1%	83,743	27
Self-Harm & Suicide	188,124	32,841	0.6%	28,207	44
False Information	439,233	1,463	0.1%	1,277	12
Impersonation	440,437	14,557	0.3%	14,381	3
Spam	1,981,115	1,002,278	18.6%	645,238	2
Drugs	368,732	241,227	4.5%	166,562	55
Weapons	115,512	13,271	0.2%	9,768	35
Other Regulated Goods	478,665	140,554	2.6%	99,768	32
Hate Speech	431,670	113,906	2.1%	97,621	46
Terrorism & Violent Extremism	119,297	2,574	0.1%	2,136	45

Analysis of Content and Account Violations

Our overall reporting and enforcement rates remained fairly similar to the previous six months. This cycle, we saw an approximate 10% increase in total content and account reports.

The Israel-Hamas conflict began during this period, and as a result we saw an uptick in violative content. Total reports related to hate speech increased by ~61%, while total content enforcements of hate speech increased by ~97% and unique account enforcements increased by ~124%. Terrorism & Violent extremism reports and enforcements have also increased, though they comprise <0.1% of the total content enforcements on our platform. Our Trust & Safety teams continue to remain vigilant as global conflicts arise in order to help keep Snapchat safe. We have also expanded our transparency report to include more information at a global and country-level regarding the total reports, content enforced, and unique accounts enforced for violations of our Terrorism & Violent Extremism policy.

Combating Child Sexual Exploitation & Abuse

Sexual exploitation of any member of our community, especially minors, is illegal, abhorrent, and prohibited by our Community Guidelines. Preventing, detecting, and eradicating Child Sexual Exploitation and Abuse (CSEA) on our platform is a top priority for Snap, and we continually evolve our capabilities to combat these and other crimes.

Sexual exploitation of any member of our community, especially minors, is illegal, abhorrent, and prohibited by our Community Guidelines. Preventing, detecting, and eradicating Child Sexual Exploitation and Abuse (CSEA) on our platform is a top priority for Snap, and we continually evolve our capabilities to combat these and other crimes.

We use active technology detection tools, such as PhotoDNA robust hash-matching and Google's Child Sexual Abuse Imagery (CSAI) Match to identify known illegal images and videos of child sexual abuse, respectively, and report them to the U.S. National Center for Missing and Exploited Children (NCMEC), as required by law. NCMEC then, in turn, coordinates with domestic or international law enforcement, as required.

In the second half of 2023, we proactively detected and actioned 59% of the total child sexual exploitation and abuse violations reported. This reflects a 39% total decrease from the previous period due to enhancements in Snapchatters' options for reporting, increasing our visibility of potential CSEA sent on Snapchat.

Reason	Total Content Enforced	Total Accounts Disabled	Total Submissions to NCMEC
CSEA	1,046,296	343,865	398,736

*Note that each submission to NCMEC can contain multiple pieces of content. The total individual pieces of media submitted to NCMEC is equal to our total content enforced. We also have excluded retracted submissions to NCMEC from this number.

Self-harm and Suicide Content

We care deeply about the mental health and well-being of Snapchatters, which continues to inform our decisions to build Snapchat differently. As a platform designed for communications between and among real friends, we believe Snapchat can play a unique role in empowering friends to help each other in difficult times.

When our Trust & Safety team becomes aware of a Snapchatter in distress, they can forward self-harm prevention and support resources, and notify emergency response personnel when appropriate. The resources that we share are available on our global list of safety resources, and are publicly available to all Snapchatters.

Total Times Suicide Resources Shared
28,361

Appeals

In our previous report, we introduced metrics on appeals, where we highlighted the number of times users asked us to re-review our initial moderation decision against their account. In this report, we have expanded our appeals to capture the full range of our policy categories for account-level violations.

Policy Reason	Total Appeals	Total Reinstatements	Total Decisions Upheld	Median Turnaround Time (days) to Process Appeals
Total	520,962	20,982	473,475	2
Sexual Content	161,446	2,345	159,101	2

Transparency
Transparency Report
About
Glossary
Previous Reports
European Union
Ads Gallery
Australia
California
India
Researchers

Total	520,962	20,982	473,475	2
Sexual Content	161,446	2,345	159,101	2
Child Sexual Exploitation*	116,736	12,860	77,371	152
Harassment and Bullying	19,919	535	19,384	2
Threats & Violence	1,667	87	1,580	57
Self-Harm & Suicide	41	7	34	34
False Information	9	0	9	20
Impersonation	1,558	114	1,444	19
Spam	13,745	193	13,552	4
Drugs	192,947	4,487	188,460	0
Weapons	2,936	83	2,853	27
Other Regulated Goods	9,356	208	9,148	13
Hate Speech	484	54	430	63
Terrorism & Violent Extremism	118	9	109	46

* Stopping the spread of content or activity related to child sexual exploitation is a top priority. Snap devotes significant resources toward this goal and has zero tolerance for such conduct. Special training is required to review CSE appeals, and there is a limited team of agents that handles these reviews due to the graphic nature of the content. In the fall of 2023, Snap implemented policy changes that affected the consistency of certain CSE enforcements; we have addressed these inconsistencies through agent re-training and quality assurance. We expect that Snap's next transparency report will reveal progress toward improving response times for CSE appeals and improving the precision of initial enforcement actions.

Ads Moderation

Snap is committed to ensuring that all ads are fully compliant with our advertising policies. We believe in a responsible and respectful approach to advertising, creating a safe and enjoyable experience for all of our users. Below we have included insight into our moderation for paid advertisements on Snapchat. Note that ads on Snapchat can be removed for a variety of reasons as outlined in Snap's Advertising Policies, including deceptive content, adult content, violent or disturbing content, hate speech, and intellectual property infringement. Additionally, you can now find Snapchat's Ads Gallery in the navigation bar of this transparency report.

Total Ads Reported	Total Ads Removed
20,204	7,258

Transparency
Transparency Report
About
Glossary
Previous Reports
European Union
Ads Gallery
Australia
California
India
Researchers

20,204	7,258

Regional & Country Overview

This section provides an overview of the enforcement of our Community Guidelines in a sampling of geographic regions. Our Guidelines apply to all content on Snapchat—and all Snapchatters—across the globe, regardless of location.

Information for individual countries, including all EU Member States, is available for download via the attached CSV file.

Download CSV

Region	Content & Account Reports	Content Enforced	Unique Accounts Enforced
North America	6,146,896	2,253,147	1,377,547
Europe	5,060,287	1,471,363	963,225
Rest of World	7,834,327	1,652,204	1,011,616
Total	19,041,510	5,376,714	3,315,759


Australia


Austria


Belgium


Brazil


Canada


Denmark

Finland

France

Germany

India

Iraq

Ireland

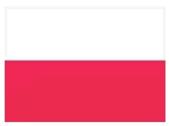
Italy

Mexico

Netherlands

New Zealand

Norway



Poland

Saudi Arabia

Spain

Sweden

Transparency
Transparency Report
About
Glossary
Previous Reports
European Union
Ads Gallery
Australia
California
India
Researchers

Saudi Arabia

Spain

Sweden

Turkey

United Arab Emir...

United Kingdom

United States

Government & Intellectual Property Removal Requests

Learn More

About Transparency Reporting

Learn More

Glossary of Transparency Report

Learn More

EXHIBIT 9

Transcript

Assembly Floor Session – 08-30-2022
05:30:28 to 05:33:15

**AM = Assembly Member*

AM Ward: Also respect your aye vote on concurrence.

Chair: Thank you, Mr. Ward. Seeing no additional comment, Clerk will open the roll. *[Bell]* All Members vote or desire to vote. All Members vote or desire to vote. All Members vote or desire to vote. Clerk will close the roll. Tally vote, Ayes 61, Nos zero. Senate amendments are concurred in. This is file item 338 AB 2273. Clerk will read.

Clerk: A summary of Bill 2273 by Senate Member Wicks and others an act relating to consumer privacy.

Chair: Ms. Wicks.

AM Wicks: Thank you, Mr. Speaker, and Members. AB 2273 will establish the California Age-Appropriate Design Code to help create safer online experiences for kids in our state. Senate amendments reflect numerous conversations with stakeholders and ensure that California youth receive the same robust protection as their peers in the UK and Europe. They include language that will limit enforcement to the attorney general, create robust penalties, and ensure businesses in substantial compliance with the Age-Appropriate Design Code have an opportunity to remedy violations prior to being subject to civil penalties. Should this Bill become law, California will lead the way in making the digital world safer for for American children and take a major step towards creating a global standard for the protection of youth online. That is the side of the story that I want California to be on. I respectfully ask for an aye vote.

Chair: Thank you, Ms. Wicks. Mr. Cunningham.

AM Cunningham: Thank you, Mr. Speaker, I'll be quick. I rise as a proud joint author of AB 2273. I think this is the best bill protecting kids online that is going to come before this legislature, and I respectfully ask for a strong aye vote.

Chair: Thank you, Mr. Cunningham. And Mr. Gabriel.

AM Gabriel: Thank you, Mr. Speaker, I also rise in support of AB 2273. I want to complement our colleagues Assembly Woman Wicks and Assembly Member Cunningham for very skillfully putting together a really important bill here. And we spent a lot of time in the privacy Committee this year talking about all of the challenges that young people face online.

We heard from so many parents and so many young people about the dangers of navigating the online world. This is a very thoughtful Bill that takes a consumer protection approach. It's going to have a big impact here in the state of California and beyond, far, far beyond. Respectfully urge an aye vote on AB 2273.

Chair: Thank you, Mr. Gabriel. Seeing no other members seeking recognition on this item, Clerk will open the roll. *[Bell]* All members vote who desire to vote.

EXHIBIT 10

Transcription of Legislating Data Privacy Streams

00:00:12 David Strauss Welcome to another episode of Data Privacy Unlocked. My name is David Strauss. With me today is California Assemblymember Buffy Wicks. Assemblymember Wicks is the primary sponsor of the 2022 California Age Appropriate Design Code Act, a first in the nation law focused on online child safety issues. The Act is set to go into effect on July 1st, 2024, but it is already causing a lot of attention as you might already know. Assemblymember Wicks, thank you for joining us today.

00:00:44 Buffy Wicks Thank you so much for having me.

00:00:46 David Strauss So, maybe I can kind of start from the beginning. That's always a good place to begin. How did you get interested in running the AADC?

00:00:54 Buffy Wicks Well, you know, I'd done some work in the space prior. I did a bill previous to this, the Kids Act, that was looking at more direct regulation of algorithms as it pertained to, you know, you stick your kid on Youtube and watching, you know, Thomas the Train videos, and you come back 40 minutes later and they're watching trainwrecks, or something like that, right? And how those algorithms can move you into different directions. That bill did not end up making it out of the process, but we had really interesting conversations in the Privacy Committee. We have a Privacy Committee here in California. And it's obviously bipartisan as all of our committees are. But really its comprised of parents, you know, and my joint co-author on this bill, Jordan Cunningham is a dad of four, and I have two girls. His kids are a little bit older than mine, so they're kind of in the throes of being teenagers in the era of social media. My kids are six and two, and so they're, I'm looking down the kind of, my future seeing that come towards them. And really we just kind of came together as parents around this notion that we just need strong regulatory environment for our kids, you know. And my kids, they're not going to be Luddites, they're digital natives, you know. My daughter is six years old and she's like, "When do I get to get a phone?" And I'm like, "A long time from now is when you're going to get a phone." But they obviously see us with phones and they're, you know, they're fluent on it. And I just want to create a better environment, you know, and for all of our kids, and you know, I don't know if you saw yesterday, the CDC came out with some pretty alarming research around kids mental health. Sixty percent of young girls are, have experienced sadness and hopelessness over the past year. Sixty percent, you know, suicidal ideation is up. Suicidal attempts are up. I mean, all these things right now. I don't know if we can completely attribute all that to social media, right? I know that's a conversation that happens, but it

certainly does have an impact. And you know, we need to wrap our heads around this a little bit more. So really I just came to this issue set more as a parent than anything else, as did many of my colleagues who wanted to work on this bill. And in California, you know, Jordan Cunningham is the joint author. And I also had a woman named Coddy Petrie-Norris, who is a member Norris. I represent a very progressive district, Jordan is a Republican and Coddy is sort of a moderate Democrat. And so those are kind of the three parties in the California state legislature. And all three of us just came to it just trying to solve a problem in an era of very divisive politics, we just wanted to solve a problem. So that was, that's what kind of birthed Age-Appropriate Design. Obviously we stole it from the UK, because we like to think that we created everything here in California but we also try to steal other people's good ideas too.

00:03:36 David Strauss Let me ask you about the, where you landed on that one. I mean you say a lot of like unpack, but the UK, for listeners out there, some may be familiar, some may not, the UK has UK Age-Appropriate Design care, it's the same name of the bill. That goes into effect first, and then, how does it happen that you guys become, I mean did you do your own research, is there organizations come to you with that, what's the, what's the process that happens?

00:04:01 Buffy Wicks Yeah, so, prior to being an elected official in 20- sort of 15 and 16, I was working with an organization called Common Sense Media. And we were really working on some of these issues. So I had familiarity with it, and as I mentioned in prior policy working it. I think it sort of developed a reputation of someone who is willing to, you know, tackle some tougher issues as pertaining to tack, specifically around a kids' lens. And some of the folks that worked at Common Sense Media and are working with an organization called Five Rights, Yvonne Kidron, the Baroness, is the one who started that organization and she was really the chief architect of the bill that become law in the UK. And so through various, you know, ways we connected and she flew out here to California and we started talking about it and kind of plotting and scheming and how we thought if we, if they could pass this in the UK we could pass it here in California. Chances are other states may follow suit and maybe our federal government. And if even if no other policies follow suit, other, you know, legislation, certainly if we create a floor of behavior here for tech companies in California and one in the UK, then a lot of the companies may follow suit anyway, because they don't want, you know, it's, it's easier for them if they just have the standard they have to reach in California and the UK, that would work as opposed to having a standard in California that's different than the standard in Nevada, you know? So we thought, you know, if we're able to kind of have a, you know, a marquee law in the EU and a marquee law, although UK's not in the Union anymore, but in Europe,

and a marquee law here in California we could actually potentially create some global change on the issue.

00:05:43 David Strauss You mentioned right, right before we started, that you're aware that other states are in fact, you know, looking AADC bills. It sounds like that was very intentional on your part.

00:05:51 Buffy Wicks Yeah, and, you know, this is not new in California, right? We created industry standards around car emissions, you know, other things then I think follow suit in other places. And I think it's also just interesting because we are, like, home of the tech industry? You know, a lot of, obviously Silicon Valley is here. A lot of my constituents work in the tech industry. I represent the East Bay, Oakland, Berkeley and Richmond, so you know we have a lot of the tech industry in my district. And so we've had a lot of these conversations around privacy regulation, tech regulation, anti-trust work, etc. in the California legislature for years. You know, we've passed landmark legislation four years ago I think it was, we did ballot measure work two years ago to create a regulatory agency and privacy. We have a Privacy Committee, I don't think a lot of other state legislatures have a Privacy Committee that's focused on this. So we have, I think, a history here in California of doing this type of stuff and then we also have, like, a really good bipartisan group of people who care about it. And really just want to kind of put party ideology aside and try to think through how we can actually solve the problem.

00:07:02 David Strauss And now all I see, one of these that really stands out when you read about the AADC is that it passed without a single no vote at any point. Of any committee or in the Assembly or in the Senate. I think that speaks volumes to how this issue resonates across party lines.

00:07:19 Buffy Wicks I mean, that was my experience, and we have opposition from the tech industry and opposition from trade association groups and we talked a lot with the opposition. But we also spent a lot of time, I as a legislator and my colleagues who were, who were joint authors on the bill, talking to our colleagues about it. And I think again coming in kind of as parents trying to get stuff done to protect our kids, I think was sort of the basis of this. We also had a young woman named Amy who was 15 or 16 at the time testifying in the committees about her experience as a teenager navigating social media, navigating kind of just this new world order. I think those of us, you know, I didn't have social media when I was in high school or college, really. You know, I got social media maybe when I was in my mid-twenties and so I was older. A lot of our legislators are 50, 60, 70, you know, they're older, it's an older, so they don't, I think, understand or appreciate in the same way how kids are grappling with this. So bringing her voice to the table and really centering the conversation on her experience was

also important for us. So that, so that lawmakers understood, what are our kids navigating right now? And again when you look at the data around their experience of life going through with this information onslaught coming at them on the front end and then on the back end all the information sort of being tracked by them, you know. Our number one job as lawmakers is to keep our community safe, and specifically our kids. And so, yeah, it got a lot of support across the board because I think everyone recognized we need more regulation in this space. We know we do. And, you know, if you're, you know a 45 year old person, you want to spend six hours on TikTok until three o'clock in the morning, by all means go for it. Like, you're an adult, you've made that decision. But when you're 14 years old, and you have a hard time regulating decision, the decision-making process, we should think about some parameters around maybe not sending push notifications, you know, past 9:00 pm, or whatever. Just smart things that help parents also navigate the space that we're in.

00:09:20 David Strauss Not to get personal on me, but I've got three young kids, ten, eight and six, mine are all boys. So you and I live in alternate universes. You with two girls and mine with all boys. But I know, like, for Christmas we got the boys, you know, gaming console, and it's that sort of repetitive, they keep on playing, they keep on playing, and we took one away from my oldest, and it was like, it was like taking heroin away from –

00:09:45 Buffy Wicks I know. Yeah.

00:09:47 David Strauss It's, it's kind of, it's kind of shocking when you, when you approach this, and to your point, I mean, we're of a certain age where we didn't grow up with this. I just, I just, you know, it's hard not to grow up at that age, I guess, to have all that social media influence. Yeah, sorry, I just got on my soapbox there for a minute there, but you had mentioned before, you know, the federal, right and I ask this every time I interview a state lawmaker, right, and I say, you know, do you think this is something that the federal government should do and I strong suspect that I know what your answer is. But I like to hear your point of view on, on you know, what the federal government should be doing.

00:10:25 Buffy Wicks Well I would love to see policy change at the federal level. You know, and I worked for President Obama for six years, I lived in DC for, on and off, for 15 years. I've had a lot of, I have a lot of connectivity with DC and, you know, worked on the Hill, and so, you know, I got to work on the Affordable Act and all kinds of other things that are great when our federal government actually has the ability to make change. So I would love to see federal lawmakers work on this. Obviously the president would as well. He called for essentially this

type of stuff in the State of the Union recently, which was great to hear coming from him. So I would love to see action. And I do think, you know, I mean you look at the politics of this country right now and how bifurcated the conversations are and how toxic they can be sometimes and how difficult it is to get anything done. Although there have been, certainly, some exciting things that have happened in, you know, the bipartisan guns bill last year and what the president has done, he's done, passed so many great things in terms of helping us get out of, you know, COVID and the economic hole that we're in. But having said that, it's difficult to pass anything in Washington DC, we all know that. But I think this issue is a place where we can find commonality and I, I think that because I know it because we did it in California. You know, we had a real bipartisan support on it. And so I think that that can translate in DC as well.

00:11:43 David Strauss It's interesting because, there's no reason for you to know this, but the last year Connecticut passed the privacy bill and it went to the House floor and there was an amendment proposed. And it was around children's privacy. And the interesting thing was it was a Republican who was pushing that amendment, saying this bill doesn't go far enough on children's privacy to the point that Connecticut work group and then you appear on that work group. But it really is, it's one of those ah-ha moments, because you realize that this issue really does cross party lines because everyone has kids and everyone wants to protect them.

00:12:15 Buffy Wicks That's right. Everyone wants to protect their children, and you know, I think it's, you know, from my perspective I think about it again as a parent where, you know, I want them to be fluent and literate online. I want them to be able to access and utilize the newest tools and all those other things, right? I want them to be living in a modern world with the rest of us. While at the same time, I want them to be safe and I want safeguards and I want them, you read so many stories and see so many situations and the pressures that are on them. And not to digress, but I don't know if you saw *The New York Times* did a two-year study, right, really trying to understand why the increase of suicidal ideation and attempts and saw harm in all of these things, and they think it's because, you know, we're having puberty at a younger age and having social media and a bunch of information coming at us at the same time. That's what's happening with kids and they can't handle it, right? And so it's not the direct cause of these problems but it's a piece of the conversation. And so if I as a regular, as a legislator can regulate a better environment for them to help mitigate some of those challenges, I'm going to do everything I can do to do that. As are the Republicans, I think, you know.

00:13:29 David Strauss Yeah, I, I think it, like I said, I think it does, I mean you see that across the country now, I don't know, but Republicans are, deeply red states are proposing social media regulation bills that probably would be something that, that feels very familiar to you. And some of these same themes. Let me ask you, taking from the general to the specific, then, you came in the work group this past summer in Connecticut, it was talking about children's bias among other things. And you said, I don't expect you'll remember, but you said, I listened to it over the weekend so I, it relates to one of the things that you said, that the goal of the bill was to create high privacy settings by default. Can you talk a little about what you had in mind, maybe you mentioned a few already. But what, what the, what you're hoping to encourage companies to do in that regard.

00:14:19 Buffy Wicks Yeah, and some of this, we're, we're seeing how it's unfolded in the UK. And so there's some kind of really, I think, tangible examples, right? You know, I think restrictions on DL location settings I think is important. Turning off, making it the default setting to have autoplay turned off, right? And then again, people can go on and adults can go in and change the default settings should they so choose. Some parents want to have the, the, you know, autoplay on if they're on a long car trip and they want their kid to watch, you know, Daniel Tiger for how many hours, I mean, I've been there, I know what it's like to travel with kids, right. But make the default setting not to encourage that kind of, kind of addictive behavior. But you know another example is not allowing for adults that are not in your network to direct message children under the age of 18. I don't know why you, a strange adult should be direct messaging someone who is under the age of 18. So those are some things, and then some of their stuff, you know, that has happened in the UK is just, you know, safe search is the default engine in Google now for those under the age of 18, right. The push notifications, one of the challenges that we know exists is, you know, kids are having their phone in their bedroom and it's next to their bed, and if they're getting push notifications until 10, 11, 12, one o'clock in the morning, then that's what they're doing is they're up on their phone until 10, 11, 12, one o'clock in the morning. And obviously you can say, well, it's the parents' job to take the phone out of the room. I get all that, in, in principle, but in reality, I've also been a parent and understand the challenge of trying to navigate all these things, right? So let's turn off the push notifications after a certain time. Kids need their sleep, teenagers need their sleep in particular, you know. So a lot of this is really common sense stuff that's really focused on the design of the product, not the content. And that's really important because of the Section 230, we really want to be mindful of, there's this, and I'm sure you're going to ask about it, the Net Choice lawsuit, right? But we thoroughly strongly, that this bill is really about the product design and not the content that kids are receiving. So we

think that we are in really strong legal standing in terms of that lawsuit. But it's about, it's about making the products, products that kids access, whether it be apps or websites, etc., they're by design, by default created with kids in mind. And right now they're not, and you know, I spent a lot of time talking to tech companies throughout the process of this bill. I sat down and talked to Meta and it was like three moms at Meta who were talking to me about this sort of stuff, right? They want their kids to be safe, too, you know. And so I think it's a question of, is kid safety like, priority number 45 that kind of doesn't get discussed very often in the C-Sweet meetings or is it items number one, two and three, right? Are we making, and the goal of the bill is to put it at the top of the priority list so that we're forcing the companies to be more mindful about the products that they are creating in terms of kids accessing them.

00:17:12 David Strauss So let me ask you, there are a number of things to ask you about, about their response. One thing that kind of stuck out at the beginning was, at the age threshold of under 18, CAPA, the federal bill Privacy Protection Act is under 13. I know having been part of the process before, there's a big fight over like, what that age should be, should it be under 16, should it be, you know, under 17. How did you guys land on under 18?

00:17:38 Buffy Wicks I, because that's the age by which you become an adult, when you're 18. And when you're under 18, you're not an adult, right? And there's a reason for that, you know, and I think, you know, we were pushed to the, you know, 13 and, you know, but 13, 14 year olds like, they need protections too. Are we saying that they're ready to be adults? We're not, right? So we felt strongly that 18 was the right standard, especially for a bill like this, that it's, the right type of regulation that says allow for kids to be online and experience all these things and navigate the world, but we just want them to do it safely. So you know, that was one of, the tech industry wanted to bring the age down, but you know, again, when we had Amy speak, she's, she was I think 16 at the time when she was talking about her experiences and she was begging for regulation. And you hear this more often from teens. There's, there's different, you know, emerging movements from teenagers who are really trying to actually get rid of their phones or take social media off of their phones. Because they understand what they're experiencing, you know. And if you have teenagers who are begging for more regulation of the space, like, let's honor them and let's put them as drivers in this process. And that's why we really try to include people like Amy in the conversation.

00:18:53 David Strauss One of these you mention is, well, and your answer was, this concept of kind of like, Connecticut and I think wrote into this AADC has a data of protection impact assessment or a data protection assessment

requirement, which is, you know, I always kind of colloquially refer to this as, like, don't create a stall grab. Right, like you should actually think through when you're designing the product. But you can probably more articulately explain what you guys were getting at with that origin.

00:19:22 Buffy Wicks

Yeah, I mean that is really important, because it sort of gets companies to think about how children under the age of 18 are going to be impacted by their product, right? Or their features or the things that they are proposing. So we want them to be thinking with intentionality as they're creating their product. I mean, listen, like, some of these product designers are, you know, these are the smartest people in the room and they're genius at a lot of the work that they do. But we really want them to be thinking about how does it impact kids. And having a systematic way companies consider new technologies with kids at the forefront of that assessment is critical to practically protecting kids from the harm that we have been seeing. You know, I mean, what if Facebook did that when creating Facebook? You know, maybe Frances Houghton wouldn't have been the whistle-blower that she is now, right? Because that, that thoughtfulness would have been on the front end. So having that kind of internal process for testing new online services and products and features, we think, is really, really important. Because it also brings them into the fold of self-regulation, right? Of them thinking through, okay, how am I as a company going to be a good actor in this space when we know we have these challenges. And I think that's also a different way of thinking about the regulation. It's not, this isn't a bill or we're being punitive and we're trying to shut down companies, we want them to be good actors in this space. And again, as I mentioned, I talked to a lot of tech companies in this process. I think a lot of them do want to be good actor, you know? It's just that there's a rung between doing the right thing but then also navigating that with getting the eyeballs on their website for the advertising dollars for the business model, you know? And so I think this forces their hand around the notion of like, how do we actually do the right thing here for kids in mind, and that's what this regulation is about. And specifically, this piece of it.

00:21:05 David Strauss

Yeah, let me ask you, I mean, you said, you guys are going to stay away from being punitive. I think one of the things that kind of sticks out when you get to the end of the bill is, the law, I should say, is there's a right to cure. And that right to cure doesn't sunset, and I think the point of that, as I understand it, was hey, we want to entice people to comply, we don't want to, you know, shut down tech, we want to, you know, incentive them.

00:21:32 Buffy Wicks

Yeah. I mean, the goal of this provision is compliance. You know, we want companies to do the right thing and to adhere to the law.

Because that's how we actually protect kids online and that is the goal, right? As I mentioned, like, I, many of my voters work in the tech industry. [Laughs] You know, and it's part of our economic resources out here. The goal is not to kill the tech industry, right? But the goal is to really get these companies to, to comply, to adhere to the law. As I mentioned it's not punitive. Now, if they continue to fail, right, you know, there are penalties and the attorney general has the ability to, to administer those and to go after them. But that's not the goal of the bill, the goal of the bill is to get them, the companies, to comply and to keep our kids safe online.

00:22:17 David Strauss Let me ask you about, some of, thornier issues in the bill and I think maybe some of it we worked out in the work group this year. There's a few places I think companies are wrestling with. One is the likely to be accessed standard. You know, and one of the criticisms that's been made against it is, well, hey, every, every company out there could be likely be accessed by someone under 18, any online website. But I, I sense that wasn't the intent of the bill, was to wrap everybody out. And what was the point of that standard, I suppose.

00:22:53 Buffy Wicks Yeah, it's not, I mean, you know, this sort of idea that likely to be accessed sort of sweeps up all companies. You know, I don't agree with that interpretation, you know. The definition of business in this bill is the same meaning as our California Consumer Privacy CCPA Act, so it's similar definitions, you know. And to be subject to the bill, the business have, there's a sort of list of requirements that they would have to meet our thresholds, they would have to meet, you know, gross revenue of over $25 million. Buy, sell or share personal information of 50,000 or more customers. And then I think the third one is receive 50 percent or more of its annual revenue from selling consumer data. So, you know, who comes into that? Facebook does. Google does, right? Companies fall into that. Who doesn't? Like, your local Chinese restaurant's website. Like, they're not, you know, it, there's a threshold here in terms of who actually is incorporated and falls into this bill and, you know. And again, we look at what's happening in the UK, you know, the age-appropriate design code in the UK was adopted there and not all companies have been impacted. So they have a similar threshold. And I looked then, because the other thing that we heard of a lot on the bill, which I suspect you're going to ask, is about the age estimation piece?

00:24:13 David Strauss My next question, in fact.

00:24:14 Buffy Wicks Sure, why don't you ask that.

00:24:16 David Strauss [Laughter] Well, you brought, you're doing my job now. [Laughter] And so, yeah, I mean, it was my next question was, this, this concept

as you set it up for the listener is, you need to do an age assurance, age verification, depending on terminology there, it gets complicated. And, you know, if you can't assure the age of the individual you default to the highest privacy settings, right? So there's this sort of like gatekeeping threshold issue that's made a lot of companies uncomfortable, I think is maybe an easy way of saying it. How do you respond to that? I mean, it's obviously something you've thought a lot about.

00:24:53 Buffy Wicks Yeah, I mean, first of all, many of these companies know exactly how old we are. Right? They have a whole engineering team devoted to this question, right? They're, Facebook is pretty sure they know how old we are, by our searches, same with Google, etc. So the companies have a very strong understanding of that and we wanted to make sure that the, the need for age estimation sort of merited the risk that, that was being put forth by the company. So for instance, Tinder, you know. They have pretty strong age verification process set forth, right? It's a dating app, you know, essentially, to be generous. And you know, you don't want 14 year olds on that site, right? Like, that is bad, we can all agree to that, right? Now the Sacramento Bee's website is a little different, you know what I mean, and so it's figuring out depending on what the company has to offer and the risk associated with it for kids, what that process will look like. But that's, this is also why the working group is so important. We have put forth in the bill the notion of the working group, which will be comprised of a number of different people delegated somewhat by the legislature, by the governor, by our regular, privacy regulatory agency here in California, to think through and provide recommendations around some of these tougher questions, so that we're being thoughtful and mindful. And again, to go back to the last question, we look at what is happening in the UK, you know. And there was a lot of fear mongering around this age estimation piece at the end of this sort of life cycle of the bill, where all of a sudden there were a couple of key people saying, "It's going to shut down the internet." You know, like, what are we, what are they doing in California, they're being crazy. But you look at the UK and guess what, the internet is not shut down. It still works. No one is requiring, you know, at every website you have to put forth your driver's license. You know, again, we're, they're going thoughtful ways of age estimation just to make sure that as people are entering their sites, as young people are entering their sites, they're being mindful of that and they're putting forth the right kind of privacy regulations. And so we will do lessons learned from there, and, and follow their lead on what's working, but also the working group is a really important piece of this.

00:27:08 David Strauss That's, help tease out the working group, because I, I mean, it's in your bill. And frankly, the tech community have been so wrapped up

with CCPA compliance that I think, something that, you know, once we finish up with that, we're going to turn to this and say, oh my goodness, right, we've got a lot, we've got a lot to work through, right? We did the CCPA. The work group, as I understand it, the idea is, it's going to be, you know, made up, you said already, a bunch of people who are nominated by various left-sided officials and they provide a report to the legislature by the end of, I think, this year, if memory serves. What's unclear to me is then, what will happen after that? Will lawmakers sit down and try to resolve some of these issues, or is that considered guidance, I suppose. Like, how's it going to work?

00:27:54 Buffy Wicks

Yeah, so the working group that was created in the bill we tasked with regularly engaging relevant stake holders including the legislature and others, the governor and others, you know, in the children's privacy space and making recommendations to the legislature every two years that help us think through how technology is changing and how it's impacting children. You know, we recognize that technology moves faster than the legislative process. We are not known for our speed. So the working groups will all be kind of identify gaps and evaluate how children can be further prioritized in the design and in development and implementation of new online products and services and features and other kind of tasks necessary to ensure that, that the law is effective, right? And so it's really to kind of provide that kind of feedback that we really need, you know? No offense to myself or my colleagues, but many of us are not tech experts. And so we need the, that type of guidance. And really that type of guidance will also serve as a model for companies as they're thinking through their assessments as companies, of what they should be mindful of and how they should be thinking about this. You know, and the AG has the ability, and I think will ask for companies to provide those assessments. You know, and I can only speak to our current AG, attorney general Rob Bonta. He's been a leader in this space. And so I expect he will be kind of a full participant and really trying to be active in ensuring that companies are compliant. And again, not in a punitive way, but in a way that just ensures that they adhere to the law. So with the working group and the assessments and the attorney general's role and the legislature taking input from the working group, we really tried to make this kind of a holistic approach around thinking through what could be pretty complex and ever evolving dynamics, right? And as you mentioned, I know in California we're still figuring out sort of implementation of laws prior, but I think this space is kind of, it is what's on the horizon as the next thing that we need to focus on.

00:29:55 David Strauss So this, actually, work group will push out guidance for companies to, to adhere to, to be able to ensure that they are in, in compliance, is that the idea? Okay.

00:30:07 Buffy Wicks Yeah.

00:30:08 David Strauss So, you mentioned before the Net Choice law. It was shortly after the law passed, a few months after the law passed, Net Choice brought a lawsuit against the AG's office, if memory serves, on the cases that the law is unconstitutional. Sounds like you disagree. [Laughter]

00:30:29 Buffy Wicks Yeah. I mean, I'm obviously aware of the lawsuit and disagree with the assertion that the age appropriate design bill here are no wise unconstitutional. I mean we had our legislative counsel draft the bill, I went through an exhaustive legislative process. It went through our Judiciary Committee, you know, who are a team of lawyers who look at exactly these types of questions. The bill does not regulate content and we, you know, we were very intentional about staying away from provisions that we thought violate Section 230. So I'm confident that the bill, you know, will hold up against the lawsuit. And I'm not surprised by the lawsuit, right? It's, it's a tech industry trade association group who doesn't want to be regulated.

00:31:12 David Strauss Last question I'm going to ask you then is, what, what are you working on today? What's next? What's the next thing –

00:31:19 Buffy Wicks Oh, we, David we are plotting and scheming on some very exciting things in this space.

00:31:23 David Strauss Is that all you're going to give me? [Laughter] Why are you scheming?

00:31:28 Buffy Wicks That have yet to be introduced, but will be introduced soon. And I'm happy to come back and chat with you about those. [Laughter]

00:31:34 David Strauss Okay. Well that's, that's very a lead in some respects, that you'll be working on some new things. We will be anxiously waiting, so many of us out here are, you know, are strangely our lives are completely dependent on what lawmakers do and what they come up with. [Laughter] And try to navigate all these wonderful things. So, I'm just, you know, thanking you and also just give you one last chance if there's any parting thoughts you want to leave everybody with?

00:32:05 Buffy Wicks No, I mean, I just think, you know, this is a space that I think, you know, more intentionality. I like that this is a space that does not get caught up in party ideology. That this is a space where we can actually put forth kind of common sense measures that help our kids. And I think that is something that everyone can rally around. I think

that's what you've seen here in California and hopefully what you see in other state legislatures. And you know, I personally welcome Democrats and Republicans trying to work together to solve these problems. And I say that as, like, probably one of the most progressive members of the state legislature, represent Berkeley, a very progressive district. But know that if we're going to solve our problems we've really got to work together, maybe that's what this represents.

00:32:44 David Strauss Well, certainly. Thank you so much for coming on the program today. We will now, we will be anxious to see what comes next from you. We'll all be paying close attention.

00:32:53 Buffy Wicks Great, thanks for having me.

[END OF TRANSCRIPT]

EXHIBIT 11

Pew Research Center

FOR RELEASE DECEMBER 11, 2023

Teens, Social Media and Technology 2023

YouTube, TikTok, Snapchat and Instagram remain the most widely used online platforms among U.S. teens

BY *Monica Anderson, Michelle Faverio and Jeffrey Gottfried*

FOR MEDIA OR OTHER INQUIRIES:

Monica Anderson, Director, Internet and Technology
Jeffrey Gottfried, Associate Director
Haley Nolan, Communications Manager
202.419.4372
www.pewresearch.org

RECOMMENDED CITATION

Pew Research Center, December 2023, "Teens, Social Media and Technology 2023"

How we did this

Pew Research Center conducted this study to better understand teens' use of digital devices, social media and other online platforms.

The Center conducted an online survey of 1,453 U.S. teens from Sept. 26 to Oct. 23, 2023, through Ipsos. Ipsos recruited the teens via their parents, who were part of its KnowledgePanel. The KnowledgePanel is a probability-based web panel recruited primarily through national, random sampling of residential addresses. The survey was weighted to be representative of U.S. teens ages 13 to 17 who live with their parents by age, gender, race and ethnicity, household income, and other categories.

This research was reviewed and approved by an external institutional review board (IRB), Advarra, an independent committee of experts specializing in helping to protect the rights of research participants.

Here are the questions used for this analysis, along with responses, and its methodology.

A note on terminology

Our September-October 2023 survey asked about "Twitter (recently renamed to 'X')." The terms **Twitter** and **X** are both used in this report to refer to the same platform.

Teens, Social Media and Technology 2023

YouTube, TikTok, Snapchat and Instagram remain the most widely used online platforms among U.S. teens

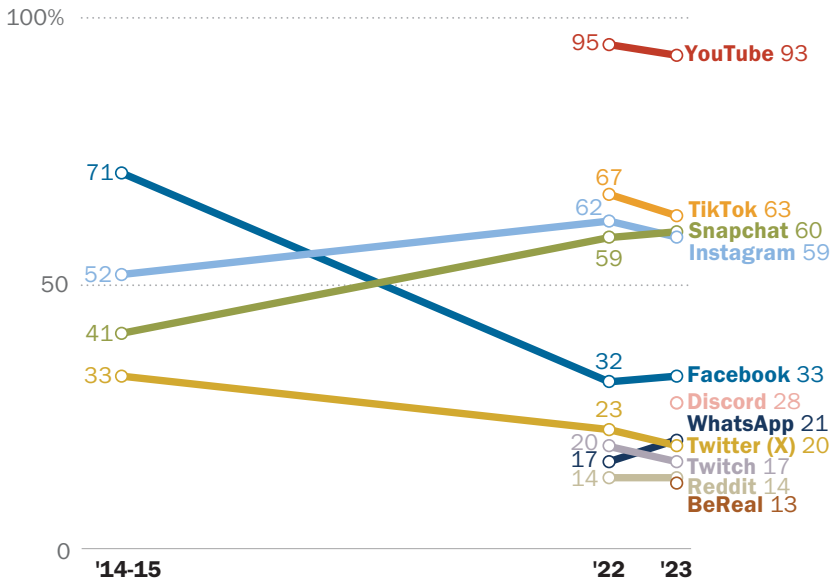
Despite negative headlines and growing concerns about social media's impact on youth, teens continue to use these platforms at high rates – with some describing their social media use as "almost constant," according to a new Pew Research Center survey of U.S. teens.

The survey – conducted Sept. 26-Oct. 23, 2023, among 1,453 13- to 17-year-olds – covered social media, internet use and device ownership among teens.

Here's a look at the key findings related to online platforms:

YouTube continues to be top platform among teens, followed by TikTok, Snapchat and Instagram

% of U.S. teens ages 13 to 17 who say they ever use the following apps or sites



Note: Those who did not give an answer are not shown.
Source: Survey of U.S. teens conducted Sept. 26-Oct. 23, 2023.
"Teens, Social Media and Technology 2023"

PEW RESEARCH CENTER

YouTube continues to dominate. Roughly nine-in-ten teens say they use YouTube, making it the most widely used platform measured in our survey.

TikTok, Snapchat and Instagram remain popular among teens: Majorities of teens ages 13 to 17 say they use TikTok (63%), Snapchat (60%) and Instagram (59%). For older teens ages 15 to 17, these shares are about seven-in-ten.

Teens are less likely to be using Facebook and Twitter (recently renamed X) than they were a decade ago: Facebook once dominated the social media landscape among America's youth, but the share of teens who use the site has dropped from 71% in 2014-2015 to 33% today. Twitter, which was renamed X in July 2023, has also seen its teen user base shrink during the past decade – albeit at a less steep decline than Facebook.

Teens' site and app usage has changed little in the past year. The share of teens using these platforms has remained relatively stable since spring 2022, when the Center last surveyed on these topics. For example, the percentage of teens who use TikTok is statistically unchanged since last year.

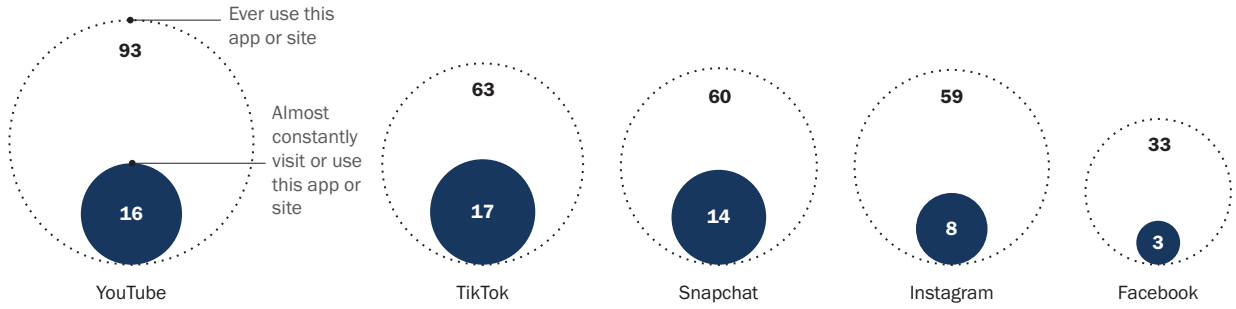
And for the first time, we asked teens about using BeReal: 13% report using this app.

How often do teens visit online platforms?

In addition to asking teens about the types of platforms they use, we also asked them how often they use five specific platforms: YouTube, TikTok, Snapchat, Instagram and Facebook.

Nearly 1 in 5 teens say they're on YouTube, TikTok 'almost constantly'

% of U.S. teens ages 13 to 17 who say they …



Note: Those who did not give an answer or gave other responses are not shown.
Source: Survey of U.S. teens conducted Sept. 26-Oct. 23, 2023.
"Teens, Social Media and Technology 2023"

PEW RESEARCH CENTER

YouTube, the most widely used platform measured in the survey, is also frequently visited by its users. About seven-in-ten teens say they visit the video-sharing platform daily, including 16% who report being on the site almost constantly.

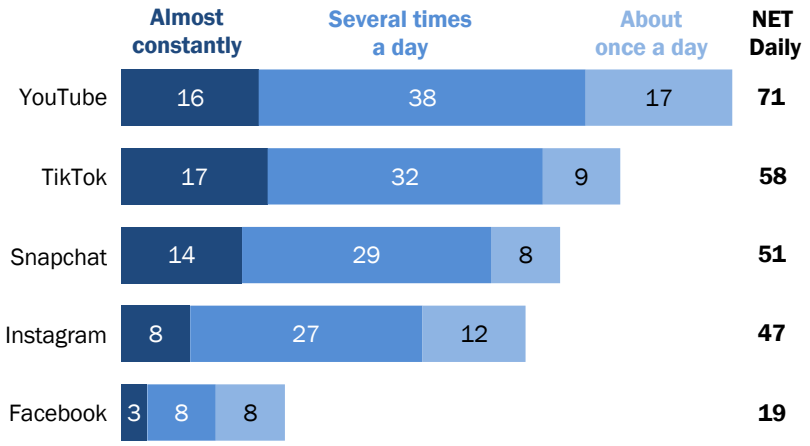
At the same time, 58% of teens are daily users of TikTok. This includes 17% who describe their TikTok use as almost constant.

About half of teens use Snapchat and Instagram daily. A somewhat larger share reports using Snapchat almost constantly compared with Instagram (14% vs. 8%).

Far fewer teens say they use Facebook on a daily basis (19%), with only 3% saying they are on the site almost constantly.

A majority of teens visit YouTube, TikTok daily

% of U.S. teens ages 13 to 17 who say they visit or use the following apps or sites ...



Note: Those who did not give an answer or gave other responses are not shown.
Source: Survey conducted Sept. 26-Oct. 23, 2023.
"Teens, Social Media and Technology 2023"

PEW RESEARCH CENTER

Taken together, a third of teens use at least one of these five sites almost constantly – which is similar to what we found last year.

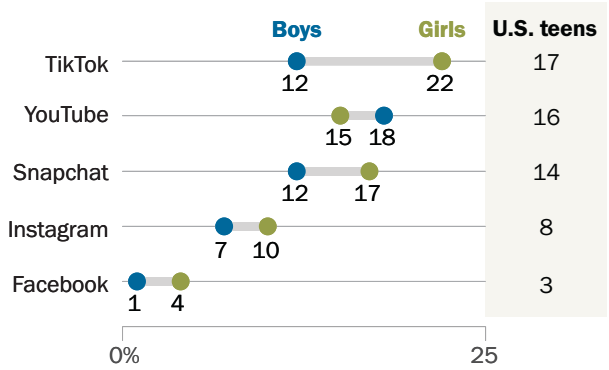
By gender

Teen girls are more likely than boys to say they almost constantly use TikTok (22% vs. 12%) and Snapchat (17% vs. 12%).

But there are little to no differences in the shares of boys and girls who report almost constantly using YouTube, Instagram and Facebook.

Teen girls far more likely than boys to say they use TikTok almost constantly

*% of U.S. teens ages 13 to 17 who say they visit or use the following apps or sites **almost constantly***



Note: Those who did not give an answer or gave other responses are not shown.
Source: Survey of U.S. teens conducted Sept. 26-Oct. 23, 2023. "Teens, Social Media and Technology 2023"

PEW RESEARCH CENTER

By race and ethnicity

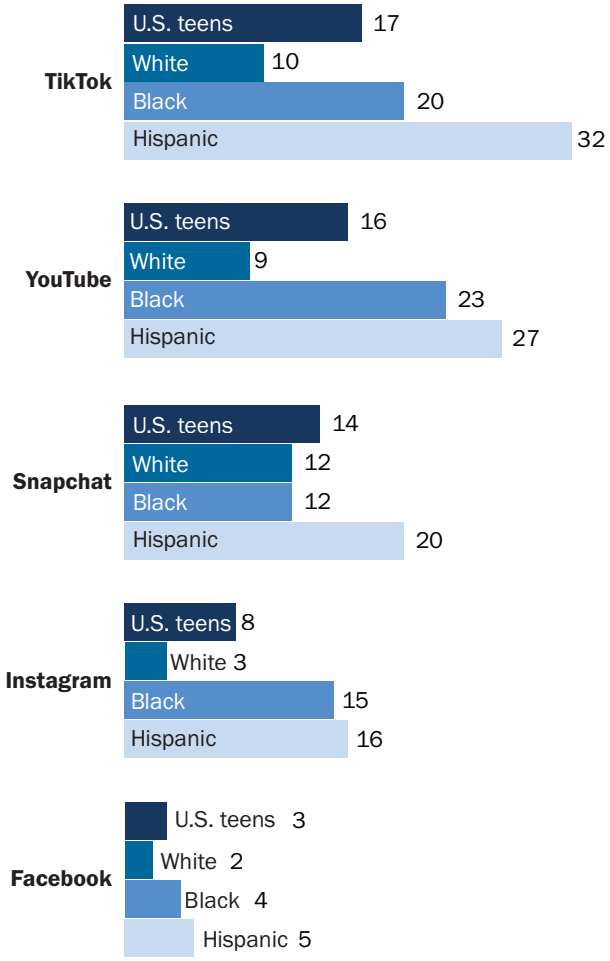
We also see differences by race and ethnicity in how much time teens report spending on these platforms.

Larger shares of Black and Hispanic teens report being on YouTube, Instagram and TikTok almost constantly, compared with a smaller share of White teens who say the same.[1]

Hispanic teens stand out in TikTok and Snapchat use. For instance, 32% of Hispanic teens say they are on TikTok almost constantly, compared with 20% of Black teens and 10% of White teens.

About 1 in 3 Hispanic teens say they're almost constantly on TikTok

% of U.S. teens ages 13 to 17 who say they visit or use the following apps or sites ***almost constantly***



Note: White and Black teens include those who report being only one race and are not Hispanic. Hispanic teens are of any race. Those who did not give an answer or gave other responses are not shown.
Source: Survey of U.S. teens conducted Sept. 26-Oct. 23, 2023. "Teens, Social Media and Technology 2023"

PEW RESEARCH CENTER

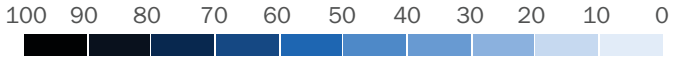
[1] There were not enough Asian teens in the sample to be broken out into a separate analysis. As always, their responses are incorporated into the general population figures throughout the report.

How use of online platforms differs across demographic groups

While some sites are commonly used among all teens, there are some differences by gender, race and ethnicity, age, and household income.

Teen girls more likely than boys to use several sites, including Instagram, Snapchat

% of U.S. teens ages 13 to 17 who say they ever use the following apps or sites



	YouTube	TikTok	Snapchat	Instagram	Facebook	WhatsApp	Twitter (X)	Reddit	BeReal
U.S. teens	93	63	60	59	33	21	20	14	13
Boys	96	59	56	53	29	21	21	18	8
Girls	91	68	65	66	36	21	19	10	19
White	92	57	62	56	34	14	18	13	16
Black	94	80	66	69	37	20	28	16	10
Hispanic	96	70	59	62	31	28	19	13	7
Ages 13-14	94	58	49	45	24	20	12	10	13
15-17	92	67	67	68	38	21	25	16	13
Urban	91	67	59	65	35	28	21	14	7
Suburban	94	62	58	58	28	22	22	16	15
Rural	94	62	64	55	40	12	16	10	14
Household income									
<$30,000	93	71	65	60	45	20	19	14	7
$30K-$74,999	93	66	58	59	41	25	22	14	9
$75,000+	93	61	60	59	27	19	19	14	16

Note: Not all numerical differences between groups shown are statistically significant. White and Black teens include those who report being only one race and are not Hispanic. Hispanic teens are of any race. Those who did not give an answer are not shown.
Source: Survey of U.S. teens conducted Sept. 26-Oct. 23, 2023.
"Teens, Social Media and Technology 2023"

PEW RESEARCH CENTER

By gender

Teen girls are more likely than teen boys to say they use Instagram (66% vs. 53%). BeReal, TikTok, Snapchat and Facebook also are more commonly used by teen girls.

On the other hand, teen boys are more likely than teen girls to use Discord (34% vs. 22%) and Twitch (22% vs. 11%). Similarly, a larger share of boys than girls use Reddit and YouTube.

By race and ethnicity

Eight-in-ten Black teens report using TikTok, compared with 70% of Hispanic teens and 57% of White teens. Racial and ethnic gaps are also present in use of Twitter: Black teens are more likely than Hispanic or White teens to be Twitter users.

When it comes to WhatsApp, Hispanic teens are more likely than Black or White teens to say they use the messaging platform.

BeReal is the only platform asked about that White teens are more likely to use than Black or Hispanic teens.

By age

Older teens are more likely than younger teens to use many of the platforms asked about, including Instagram, Snapchat, Facebook, Twitter, TikTok and Reddit. For example, while 68% of teens ages 15 to 17 say they use Instagram, this share drops to 45% among teens ages 13 and 14.

By household income

While fewer teens overall are using Facebook, our surveys consistently show that usage remains higher among teens in lower-income households. For example, 45% of teens in households earning less than $30,000 a year say they use Facebook, compared with 27% of those whose annual household income is $75,000 or more.

Income gaps are also present in TikTok use: Larger shares of teens in lower-income households are users compared with those in the highest-income households (71% vs. 61%).

In comparison, BeReal is more commonly used among teens in households earning $75,000 or more a year. Some 16% of teens in this category say they use this app, compared with about one-in-ten whose annual household income falls below $75,000.

How much time are teens spending online?

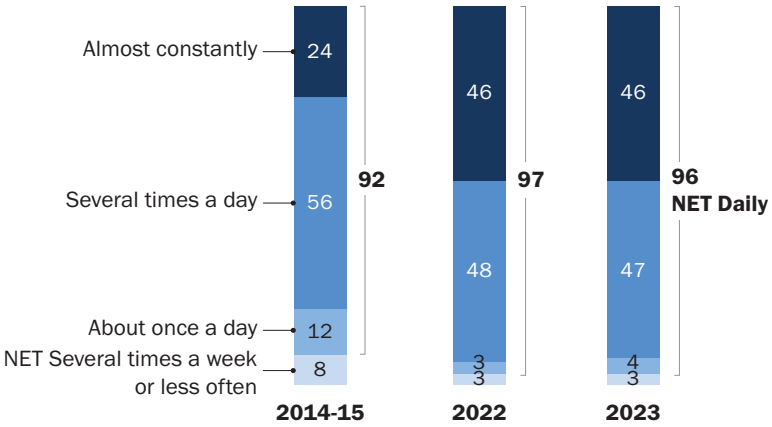
In addition to asking teens about their social media use, we also examined the amount of time they report spending online.

Nearly half of teens say they use the internet "almost constantly." This is on par with what we found last year, but roughly double the 24% who said this in the 2014-2015 survey.

Overall, more than nine-in-ten say they use the internet at least daily.

The share of teens who say they are online 'almost constantly' has roughly doubled since 2014-2015

% of U.S. teens ages 13 to 17 who say they use the internet ...



Note: Figures may not add up to NET values due to rounding. Those who did not give an answer are not shown.
Source: Survey of U.S. teens conducted Sept. 26-Oct. 23, 2023.
"Teens, Social Media and Technology 2023"

PEW RESEARCH CENTER

By race and ethnicity

As was true in previous Center surveys, the amount of time teens report spending online varies by race and ethnicity.

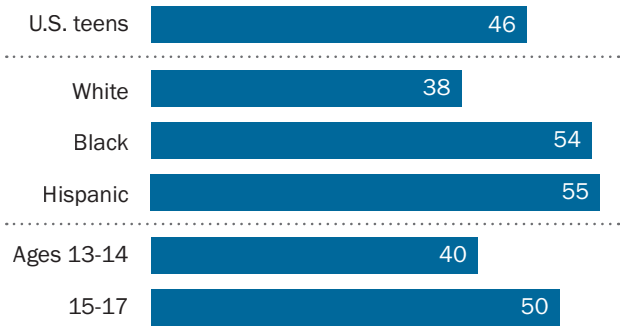
While 55% of Hispanic and 54% of Black teens report being on the internet almost constantly, the share drops to 38% among White teens.

By age

Older teens ages 15 to 17 are somewhat more likely than younger teens to be near-constant internet users (50% vs. 40%).

Black, Hispanic teens more likely than White teens to say they are online almost constantly

*% of U.S. teens ages 13 to 17 who say they use the internet **almost constantly***



Note: White and Black teens include those who report being only one race and are not Hispanic. Hispanic teens are of any race. Those who did not give an answer or gave other responses are not shown.
Source: Survey of U.S. teens conducted Sept. 26-Oct. 23, 2023. "Teens, Social Media and Technology 2023"

PEW RESEARCH CENTER

Device usage: Smartphones, computers, gaming consoles and tablets

Today's teens have several ways to go online, connect with others and find information.

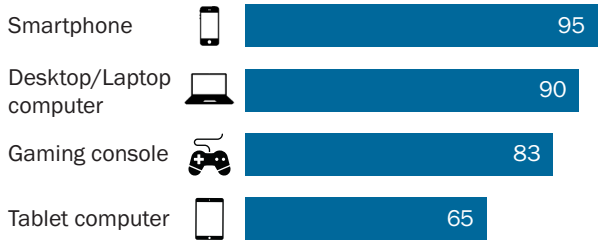
Our survey finds that most teens have or have access to a smartphone (95%), a desktop or laptop computer (90%), or a gaming console (83%). A smaller share – though still a 65% majority – say the same for tablets.

By household income

Smartphone ownership is nearly universal among teens of different genders, ages, races and ethnicities, and economic backgrounds. But having access to a home computer remains less common for those in lower-income households.

Nearly all teens in the U.S. have access to a smartphone

% of U.S. teens ages 13 to 17 who say they have access to the following devices at home



Note: Those who did not give an answer are not shown.
Source: Survey of U.S. teens conducted Sept. 26-Oct. 23, 2023. "Teens, Social Media and Technology 2023"

PEW RESEARCH CENTER

Roughly seven-in-ten teens living in households earning less than $30,000 a year (72%) say they have access to a home computer. That share rises among those whose annual household income is $30,000 to $74,999 (87%) or $75,000 and above (94%).

Tablet ownership is also less common among teens in lower-income households: 57% say they have access to a tablet at home, compared with 67% of those living in the highest-income households.

By gender

Most teen boys and girls report having access to a game console at home, but more boys say this than girls (91% vs. 75%).

Acknowledgments

This report is a collaborative effort based on the input and analysis of the following individuals. Find related reports online at pewresearch.org/internet.

Primary researchers

Monica Anderson, *Director, Internet and Technology Research*
Michelle Faverio, *Research Analyst*
Jeffrey Gottfried, *Associate Director, Research*

Research team

Emily A. Vogels, *Research Associate*
Colleen McClain, *Research Associate*
Risa Gelles-Watnick, *Research Analyst*
Olivia Sidoti, *Research Assistant*
Lee Rainie, *Former Director, Internet and Technology Research*
Eugenie Park, *Former Research Intern*

Editorial and graphic design

Kaitlyn Radde, *Associate Information Graphics Designer*
Anna Jackson, *Editorial Assistant*

Communications and web publishing

Haley Nolan, *Communications Manager*
Sara Atske, *Digital Producer*

In addition, the project benefited greatly from the guidance of Pew Research Center's methodology team: Courtney Kennedy, Ashley Amaya, Andrew Mercer, Dorene Asare-Marfo, Anna Brown, Arnold Lau and Dana Popky. This project also benefited from feedback by the following Pew Research Center staff: Drew DeSilver, Juliana Horowitz, Besheer Mohamed and John Wade. The Center gained invaluable advice in developing the questionnaire from Craig A. Anderson, Distinguished Professor of Psychology at Iowa State University; Bader Chaarani, Assistant Professor of Psychiatry at University of Vermont; and Dmitri Williams, Professor at University of Southern California's Annenberg School for Communication and Journalism.

Methodology

The analysis in this report is based on a self-administered web survey conducted from Sept. 26 to Oct. 23, 2023, among a sample of 1,453 dyads, with each dyad (or pair) comprised of one U.S. teen ages 13 to 17 and one parent per teen. The margin of sampling error for the full sample of 1,453 teens is plus or minus 3.2 percentage points. The survey was conducted by Ipsos Public Affairs in English and Spanish using KnowledgePanel, its nationally representative online research panel.

The research plan for this project was submitted to an external institutional review board (IRB), Advarra, which is an independent committee of experts that specializes in helping to protect the rights of research participants. The IRB thoroughly vetted this research before data collection began. Due to the risks associated with surveying minors, this research underwent a full board review and received approval (Approval ID Pro00073203).

KnowledgePanel members are recruited through probability sampling methods and include both those with internet access and those who did not have internet access at the time of their recruitment. KnowledgePanel provides internet access for those who do not have it and, if needed, a device to access the internet when they join the panel. KnowledgePanel's recruitment process was originally based exclusively on a national random-digit-dialing (RDD) sampling methodology. In 2009, Ipsos migrated to an address-based sampling (ABS) recruitment methodology via the U.S. Postal Service's Delivery Sequence File (DSF). The Delivery Sequence File has been estimated to cover as much as 98% of the population, although some studies suggest that the coverage could be in the low 90% range.[2]

Panelists were eligible for participation in this survey if they indicated on an earlier profile survey that they were the parent of a teen ages 13 to 17. A random sample of 3,981 eligible panel members were invited to participate in the study. Responding parents were screened and considered qualified for the study if they reconfirmed that they were the parent of at least one child ages 13 to 17 and granted permission for their teen who was chosen to participate in the study. In households with more than one eligible teen, parents were asked to think about one randomly selected teen and that teen was instructed to complete the teen portion of the survey. A survey was considered complete if both the parent and selected teen completed their portions of the questionnaire, or if the parent did not qualify during the initial screening.

Of the sampled panelists, 1,763 (excluding break-offs) responded to the invitation and 1,453 qualified, completed the parent portion of the survey, and had their selected teen complete the teen portion of the survey, yielding a final stage completion rate of 44% and a qualification rate of 82%. The cumulative response rate accounting for nonresponse to the recruitment surveys and

[2] AAPOR Task force on Address-based Sampling. 2016. "AAPOR Report: Address-based Sampling."

attrition is 2.2%. The break-off rate among those who logged on to the survey (regardless of whether they completed any items or qualified for the study) is 26.9%.

Upon completion, qualified respondents received a cash-equivalent incentive worth $10 for completing the survey. To encourage response from non-Hispanic Black panelists, the incentive was increased from $10 to $20 on Oct. 5, 2023. The incentive was increased again on Oct. 10, 2023, from $20 to $40; then to $50 on Oct. 17, 2023; and to $75 on Oct. 20, 2023. Reminders and notifications of the change in incentive were sent for each increase.

All panelists received email invitations and any non-responders received reminders, shown in the table. The field period was closed on Oct. 23, 2023.

Invitation and reminder dates

Invitation	Sept. 26, 2023
First reminder	Sept. 28, 2023
Second reminder	Oct. 2, 2023

Weighting

The analysis in this report was performed using separate weights for parents and teens. The parent weight was created in a multistep process that begins with a base design weight for the parent, which is computed to reflect their probability of selection for recruitment into the KnowledgePanel. These selection probabilities were then adjusted to account for the probability of selection for this survey which included oversamples of Black and Hispanic parents. Next, an iterative technique was used to align the parent design weights to population benchmarks for parents of teens ages 13 to 17 on the dimensions identified in the accompanying table, to account for any differential nonresponse that may have occurred.

Weighting dimensions

Variable	Benchmark source
Age x Gender Race/Ethnicity Census Region Metropolitan Status Education (parents only) Household Income Household Income x Race/Ethnicity Total Household Size	2023 March Supplement of the Current Population Survey (CPS)
Language proficiency	2021 American Community Survey (ACS)

Note: Estimates from the ACS are based on noninstitutionalized adults.

PEW RESEARCH CENTER

To create the teen weight, an adjustment factor was applied to the final parent weight to reflect the selection of one teen per household. Finally, the teen weights were further raked to match the demographic distribution for teens ages 13 to 17 who live with parents. The teen weights were

adjusted on the same teen dimensions as parent dimensions with the exception of teen education, which was not used in the teen weighting.

Sampling errors and tests of statistical significance take into account the effect of weighting. Interviews were conducted in both English and Spanish.

In addition to sampling error, one should bear in mind that question wording and practical difficulties in conducting surveys can introduce error or bias into the findings of opinion polls.

The following table shows the unweighted sample sizes and the error attributable to sampling that would be expected at the 95% level of confidence for different groups in the survey:

Group	Unweighted sample size	Plus or minus ...
Teens (ages 13-17)	1,453	3.2 percentage points
Boys	735	4.5 percentage points
Girls	697	4.6 percentage points
Ages 13 and 14	529	5.3 percentage points
15 to 17	924	4.0 percentage points
White, non-Hispanic	634	4.5 percentage points
Black, non-Hispanic	218	8.3 percentage points
Hispanic	454	6.1 percentage points
Household income		
<$30,000	273	8.1 percentage points
$30K - $74,999	409	6.3 percentage points
$75,000+	771	4.1 percentage points

Note: This survey includes oversamples of Black and Hispanic respondents. Unweighted sample sizes do not account for the sample design or weighting and do not describe a group's contribution to weighted estimates. Refer to the Weighting section for details.

Sample sizes and sampling errors for subgroups are available upon request.

Dispositions and response rates

The tables below display dispositions used in the calculation of completion, qualification and cumulative response rates.[3]

Dispositions	
Total panelists assigned	3,981
Total study completes (including nonqualified)	1,763
Number of qualified completes	1,453
Number of study break-offs	647
Study Completion Rate (COMPR)	**44.2%**
Study Qualification Rate (QUALR)	**82%**
Study Break-off Rate (BOR)	**26.9%**

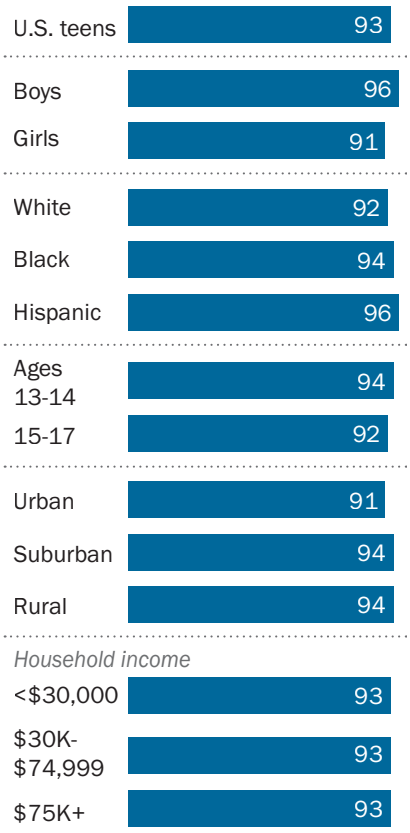
Cumulative response rate calculations	
Study-Specific Average Panel Recruitment Rate (RECR)	8.8%
Study-Specific Average Household Profile Rate (PROR)	57.2%
Study-Specific Average Household Retention Rate (RETR)	35.4%
Cumulative Response Rate	**2.2%**

[3] For more information on this method of calculating response rates, refer to Callegaro, Mario, and Charles DiSogra. 2008. "Computing response metrics for online panels." Public Opinion Quarterly.

Appendix: Teen online platform users by demographics

U.S. teen YouTube users

*% of U.S. teens ages 13 to 17 who say they ever use **YouTube***

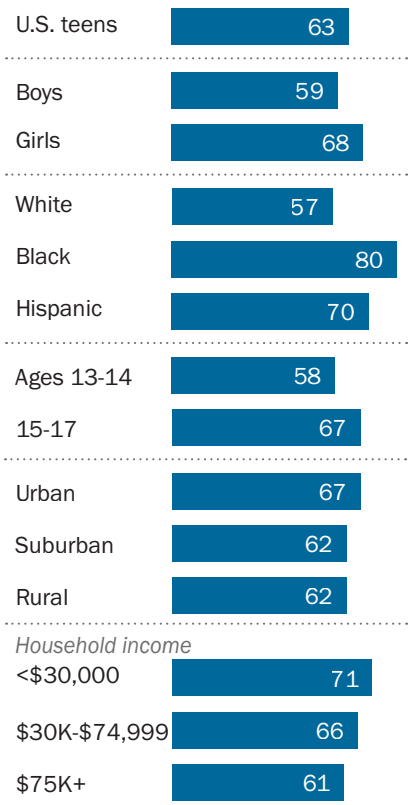


Note: White and Black teens include those who report being only one race and are not Hispanic. Hispanic teens are of any race. Those who did not give an answer are not shown.
Source: Survey of U.S. teens conducted Sept. 26-Oct. 23, 2023.
"Teens, Social Media and Technology 2023"

PEW RESEARCH CENTER

U.S. teen TikTok users

*% of U.S. teens ages 13 to 17 who say they ever use **TikTok***

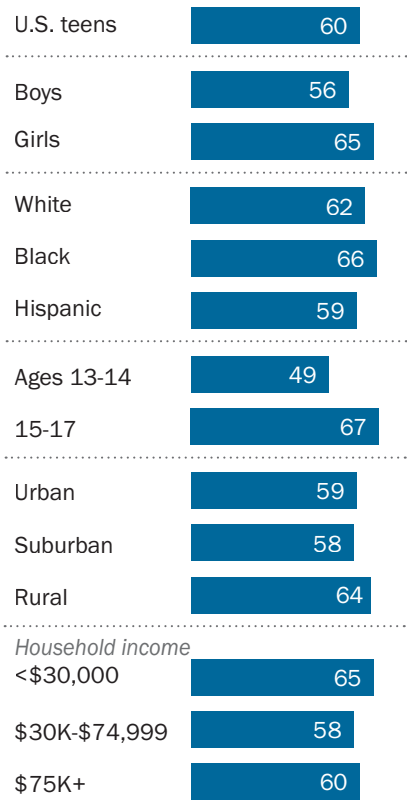


Note: White and Black teens include those who report being only one race and are not Hispanic. Hispanic teens are of any race. Those who did not give an answer are not shown.
Source: Survey of U.S. teens conducted Sept. 26-Oct. 23, 2023.
"Teens, Social Media and Technology 2023"

PEW RESEARCH CENTER

U.S. teen Snapchat users

*% of U.S. teens ages 13 to 17 who say they ever use **Snapchat***

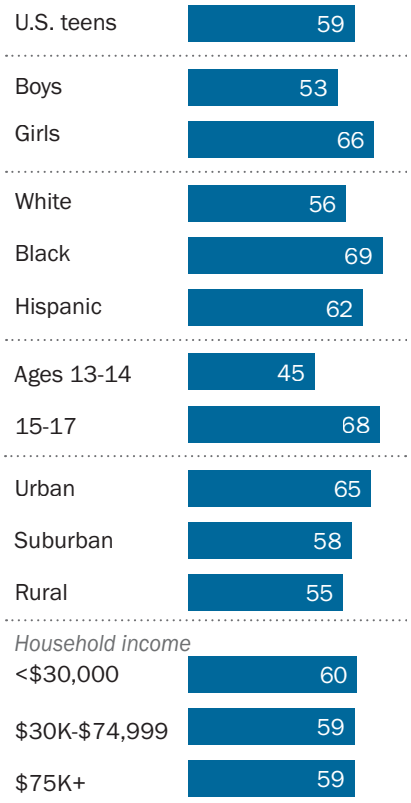


Note: White and Black teens include those who report being only one race and are not Hispanic. Hispanic teens are of any race. Those who did not give an answer are not shown.
Source: Survey of U.S. teens conducted Sept. 26-Oct. 23, 2023.
"Teens, Social Media and Technology 2023"

PEW RESEARCH CENTER

U.S. teen Instagram users

*% of U.S. teens ages 13 to 17 who say they ever use **Instagram***

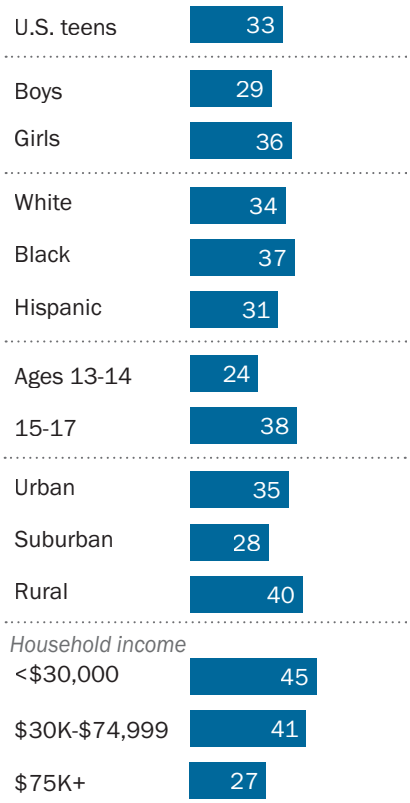


Note: White and Black teens include those who report being only one race and are not Hispanic. Hispanic teens are of any race. Those who did not give an answer are not shown.
Source: Survey of U.S. teens conducted Sept. 26-Oct. 23, 2023.
"Teens, Social Media and Technology 2023"

PEW RESEARCH CENTER

U.S. teen Facebook users

*% of U.S. teens ages 13 to 17 who say they ever use **Facebook***



Note: White and Black teens include those who report being only one race and are not Hispanic. Hispanic teens are of any race. Those who did not give an answer are not shown.
Source: Survey of U.S. teens conducted Sept. 26-Oct. 23, 2023.
"Teens, Social Media and Technology 2023"

PEW RESEARCH CENTER

Topline questionnaire

2023 PEW RESEARCH CENTER'S TEENS SURVEY
SEPTEMBER 26-OCTOBER 23, 2023
TEENS AGES 13-17
N=1,453

THE QUESTIONS PRESENTED BELOW ARE PART OF A LARGER SURVEY CONDUCTED ON THE IPSOS KNOWLEDGE PANEL. OTHER QUESTIONS ON THIS SURVEY HAVE BEEN RELEASED OR ARE BEING HELD FOR FUTURE RELEASE.

NOTE: ALL NUMBERS ARE PERCENTAGES UNLESS OTHERWISE NOTED. THE PERCENTAGES LESS THAN 0.5% ARE REPLACED BY AN ASTERISK (*). ROWS/COLUMNS MAY NOT TOTAL 100% DUE TO ROUNDING.

	Sample size	Margin of error at 95% confidence level
U.S. teens ages 13-17	1,453	+/- 3.2 percentage points

ASK ALL:
DEVICE At home, do you have or have access to…[4] **[RANDOMIZE ITEMS]**

		Yes, I do	No, I do not	No answer
a.	A smartphone			
	Sep 26-Oct 23, 2023	95	4	*
	Apr 14-May 4, 2022	95	4	*
	Sep 25-Oct 9, 2014 & Feb 10-March 16, 2015	73	27	*
NO ITEM b				
c.	A desktop or laptop computer			
	Sep 26-Oct 23, 2023	90	10	*
	Apr 14-May 4, 2022	90	10	*
	Sep 25-Oct 9, 2014 & Feb 10-March 16, 2015	87	13	*
d.	A gaming console[5]			
	Sep 26-Oct 23, 2023	83	16	1
	Apr 14-May 4, 2022	80	19	1
	Sep 25-Oct 9, 2014 & Feb 10-March 16, 2015	81	19	*
e.	A tablet computer[6]			
	Sep 26-Oct 23, 2023	65	34	1
	Sep 25-Oct 9, 2014 & Feb 10-March 16, 2015	58	42	*

[4] September-October 2014/February-March 2015 question wording was "Do you, personally, have or have access to each of the following items, or not. Do you have…?" (K3) with response options of "Yes" and "No."
[5] September-October 2014/February-March 2015 item wording was "A gaming console like an Xbox, PlayStation or Wii."
[6] September-October 2014/February-March 2015 item wording was "A tablet computer like an iPad, Samsung Galaxy or Kindle Fire." The item about tablet access was not asked in 2022.

ASK ALL:
INTREQ About how often do you use the internet, either on a computer or a cellphone?[7]

Sep 26-Oct 23, 2023		Apr 14-May 4, 2022	Sep 25 – Oct 9, 2014 & Feb 10-March 16, 2015
46	Almost constantly	46	24
47	Several times a day	48	56
4	About once a day	3	12
2	Several times a week	1	5
1	Less often	2	3
1	No answer	0	*

DISPLAY TO ALL:

Now we'd like to learn about your experiences with certain websites and mobile apps…

ASK ALL:
TSNS1 Do you ever use any of the following apps or sites? **[RANDOMIZE ITEMS]**

		Yes, I use this app or site	No, I do not use this app or site	No answer
a.	Twitter (recently renamed to "X")[8]			
	Sep 26-Oct 23, 2023	20	79	1
	Apr 14-May 4, 2022	23	77	*
	Sep 25-Oct 9, 2014 & Feb 10-Mar 16, 2015	33	66	*
b.	Instagram			
	Sep 26-Oct 23, 2023	59	41	*
	Apr 14-May 4, 2022	62	38	*
	Sep 25-Oct 9, 2014 & Feb 10-Mar 16, 2015	52	48	*
c.	Facebook			
	Sep 26-Oct 23, 2023	33	67	1
	Apr 14-May 4, 2022	32	67	*
	Sep 25-Oct 9, 2014 & Feb 10-Mar 16, 2015	71	29	*
d.	Snapchat			
	Sep 26-Oct 23, 2023	60	39	1
	Apr 14-May 4, 2022	59	41	*
	Sep 25-Oct 9, 2014 & Feb 10-Mar 16, 2015	41	59	*
e.	YouTube			
	Sep 26-Oct 23, 2023	93	6	*
	Apr 14-May 4, 2022	95	5	*

NO ITEM f.

[7] September-October 2014/February-March 2015 wording was "Overall, how often do you use the internet?" (K2) with response options of "Almost constantly," "Several times a day," "About once a day," "Several times a week," "Once a week" and "Less often." The options "Once a week" (1%) and "Less often" (2%) have been combined and presented together under "Less often" in this table.
[8] September-October 2014/February-March 2015 item wording was "Twitter."

g.	Reddit			
	Sep 26-Oct 23, 2023	14	85	1
	Apr 14-May 4, 2022	14	85	1
h.	TikTok			
	Sep 26-Oct 23, 2023	63	36	1
	Apr 14-May 4, 2022	67	33	*
i.	Twitch			
	Sep 26-Oct 23, 2023	17	82	1
	Apr 14-May 4, 2022	20	79	1
j.	WhatsApp			
	Sep 26-Oct 23, 2023	21	79	1
	Apr 14-May 4, 2022	17	82	*
k.	Discord			
	Sep 26-Oct 23, 2023	28	71	1
l.	BeReal			
	Sep 26-Oct 23, 2023	13	86	1

ASK IF USES INSTAGRAM, FACEBOOK, SNAPCHAT, YOUTUBE OR TIKTOK (TSNS1b-e,h=1):
TSNS2 Thinking about the sites or apps you use, about how often do you visit or use… **[SHOW IN SAME ORDER AS TSNS1]**

	Almost constantly	Several times a day	About once a day	Several times a week	Less often	No answer
NO ITEM a						
b. **ASK IF INSTAGRAM USER (TSNS1b=1) [N=863]:** Instagram						
Sep 26-Oct 23, 2023	14	46	20	11	8	*
Apr 14-May 4, 2022	16	44	20	12	8	*
c. **ASK IF FACEBOOK USER (TSNS1c=1) [N=469]:** Facebook						
Sep 26-Oct 23, 2023	9	25	25	18	22	1
Apr 14-May 4, 2022	7	26	24	18	24	1
d. **ASK IF SNAPCHAT USER (TSNS1d=1) [N=867]:** Snapchat						
Sep 26-Oct 23, 2023	24	48	13	8	6	*
Apr 14-May 4, 2022	25	49	11	6	8	*
e. **ASK IF YOUTUBE USER (TSNS1e=1) [N=1,355]:** YouTube						
Sep 26-Oct 23, 2023	17	40	18	15	9	*
Apr 14-May 4, 2022	20	43	18	13	6	0
NO ITEMS f-g						
h. **ASK IF TIKTOK USER (TSNS1h=1) [N=940]:** TikTok						
Sep 26-Oct 23, 2023	27	51	14	6	3	*
Apr 14-May 4, 2022	25	48	14	8	5	*
NO ITEMS i-l						

TSNS2 BASED ON ALL TEENS

	Almost constantly	Several times a day	About once a day	Several times a week	Less often	Does not use platform	No answer to TSNS1	No answer to TSNS2
NO ITEM a								
b. Instagram								
Sep 26-Oct 23, 2023	8	27	12	7	5	41	*	*
Apr 14-May 4, 2022	10	27	12	7	5	38	*	*
c. Facebook								
Sep 26-Oct 23, 2023	3	8	8	6	7	67	1	*
Apr 14-May 4, 2022	2	8	8	6	8	67	*	*
d. Snapchat								
Sep 26-Oct 23, 2023	14	29	8	5	4	39	1	*
Apr 14-May 4, 2022	15	29	7	3	5	41	*	*
e. YouTube								
Sep 26-Oct 23, 2023	16	38	17	14	8	6	*	*
Apr 14-May 4, 2022	19	41	17	12	6	5	*	0
NO ITEMS f-g								
h. TikTok								
Sep 26-Oct 23, 2023	17	32	9	4	2	36	1	*
Apr 14-May 4, 2022	16	32	9	5	4	33	*	*
NO ITEMS i-l								