February 21, 2023

The Honorable Richard J. Durbin
Chairman
Committee on the Judiciary
United States Senate
711 Hart Senate Building
Washington, D.C. 20510

Dear Chairman Durbin:

Thank you for the questions for the record from the Senate Committee on the Judiciary, Subcommittee on Competition Policy, Antitrust, and Consumer Rights hearing entitled “Big Data, Big Questions: Implications for Competition and Consumers,” held on September 21, 2021. Per your request, attached are answers for the record to your questions.

Sincerely,

Meta Platforms, Inc.

Senator Marsha Blackburn
Questions for the Record to Steve Satterfield, Vice President of Privacy & Public Policy, Facebook

1. **Please identify three distinct changes you have made to your platform to make it a safer and healthier experience for children.**

At Instagram, we have been working for a long time to help provide age-appropriate experiences on our platform; as part of that work, we recently announced some new tools and features to support keeping young people even safer on Instagram. Although we have made a number of changes, here are three recent examples:

Parental Tools. We launched tools in March 2022 to help parents and guardians guide and support their teens on Instagram. They can ask teens to enable them to view how much time their teens spend on Instagram and set time limits. We've also given teens the option to notify their parents if they report someone, giving their parents the opportunity to talk about it with them. These tools are available in our new Family Center. We worked closely with experts, parents, guardians and teens to develop Family Center, a place for parents and teens to work together on their accounts within Meta technologies, set up and use supervision tools, and access resources on how to communicate with their teens about internet use. This is just one step on a longer path—our vision for Family Center is to eventually allow parents and guardians to help their teens manage experiences across Meta technologies, all from one central place.

Family Center includes an education hub where parents and guardians can access resources from experts and review helpful articles, videos and tips on topics like how to talk to teens about social media. Parents can also watch video tutorials on how to use the supervision tools available on Instagram today. We worked closely with groups like Connect Safely and Net Family News to develop these resources, and we'll continue to add new information to Family Center's education hub. These parental supervision tools on Instagram allow parents and guardians to send invitations to their teens to initiate supervision tools, which enable them to:

- View how much time their teens spend on Instagram and set time limits;
- Set specific times during the day or week to limit their teen's use of Instagram;
- View what accounts their teens follow and the accounts that follow them;
- See more information when their teen reports an account or post, including who was reported, and the type of report;
- See a list of the accounts their teen is currently blocking on Instagram. The block list is in order of recency and denotes any users that have been blocked in the last seven days by the teen;
- See the teen's account settings specific to: (1) account privacy (public / private); (2) who can send the teen message requests (anyone / followers / no one); (3) who can add the

teen to a messaging group (everyone / only people they follow on Instagram); and (4) sensitive content controls (less / standard).

Additionally, in November 2022, we introduced updates on Facebook and Instagram to help further protect teens from online harm. For example, everyone who is under the age of 16 (or under 18 in certain countries) is now defaulted into more private settings when they join Facebook (a change we announced for Instagram in July 2021), and we encourage teens already on the app to choose these more private settings. We are also working with the National Center for Missing and Exploited Children to build a global platform for teens who are worried intimate images they created might be shared on public online platforms without their consent. This platform will be similar to work we have done to prevent the non-consensual sharing of intimate images for adults. It will allow us to help prevent a teen's intimate images from being posted online and can be used by other companies across the tech industry. In addition, we are working with Thorn and their NoFiltr brand to create educational materials that reduce the shame and stigma surrounding intimate images and empower teens to seek help and take back control if they've shared them or are experiencing sextortion.

Take A Break. We also launched "Take A Break" in certain countries to empower people to make informed decisions about how they're spending their time. If someone has been scrolling for a certain amount of time, we ask them to take a break from Instagram and suggest that they set reminders to take more breaks in the future. We show them expert-backed tips to help them reflect and reset. To make sure that teens are aware of this feature, we show them notifications suggesting they turn these reminders on.

Nudging Teens Towards Different Topics if They've Been Dwelling on One Topic for a While. Our research shows—and external experts agree—that if people are dwelling on one topic for a while, it could be helpful to nudge them towards other topics at the right moment. That's why we built an experience that will nudge people towards other topics if they've been dwelling on one topic for a while. This nudge is designed to encourage teens to discover something new and excludes certain topics that may be associated with appearance comparison.

We designed this feature because research suggests that nudges can be effective for helping people—especially teens — be more mindful of how they're using social media in the moment. In an external study on the effects of nudges on social media use, 58.2% of respondents agreed or strongly agreed that nudges made their social media experience better by helping them become more mindful of their time on-platform. Our own research shows they're working too: during a one-week testing period, one in five teens who saw our new nudges switched to a different topic.

In addition to this work, we continue to develop ways for people to verify their age on Instagram, allowing us to provide age-appropriate experiences. For example, in June 2022, we began testing new options for people on Instagram to verify their age, starting with people based in the US. If someone attempts to edit their date of birth on Instagram from under the age of 18 to 18 or over, we'll require them to verify their age using options such as uploading their ID or recording a video selfie. We're testing this so we can make sure teens and adults are in the right experience for their age group. We are also partnering with Yoti, a company that specializes in online age verification, to help ensure people’s privacy.

Our age verification tests show that our tools are working to help keep people within age-appropriate experiences. Since we began these new tools on Instagram, we’ve found that approximately four times as many people were more likely to complete our age verification requirements (when attempting to edit their date of birth from under 18 to over 18), equating to hundreds of thousands of people being placed in experiences appropriate for their age. We also were able to stop 96% of the teens who attempted to edit their birthdays from under 18 to 18 or over on Instagram from doing so. And we have found that 81% of people presented with our menu of options chose to use Yoti’s video selfie to verify their age.

Senator Chuck E. Grassley
Questions for the Record to Mr. Steve Satterfield, Vice President, Privacy & Public Policy, Facebook

1. **Facebook monetize user's data by selling targeted advertisements. In the second quarter of 2021 Facebook had revenues of $29.08 billion. It has also been reported that the average American's data was worth $164 per year to Facebook. Is it accurate that the average America's data is worth $164 per year to Facebook?**

We publicly report our Average Revenue per User ("ARPU") on Facebook, both for advertising and other revenue, broken out by geographic region. ARPU is a revenue-based metric and not a valuation of people's data. As stated in our public financial filings, we define ARPU as our total revenue in a given geography during a given quarter, divided by the average of the number of monthly active users in the geography at the beginning and end of the quarter. In the U.S. and Canada, Facebook's ARPU from advertising was $58.77 in the fourth quarter of 2022.

We also report the Average Revenue per Person ("ARPP") across Meta's family of apps, both for advertising and other revenue. As with ARPU, ARPP is a revenue-based metric and not a valuation of people's data. As stated in our public financial filings, we define ARPP as our total revenue during a given quarter, divided by the average of the number of MAP at the beginning and end of the quarter. Meta's ARPP from advertising across its family of apps was $8.63 in the third quarter of 2022.

For more information, please see our latest earnings presentation (https://s21.q4cdn.com/399680738/files/doc_financials/2022/q4/Earnings-Presentation-Q4-2022.pdf).

2. **There is debate over whether Big Data should be regulated through the lens of consumer protection and privacy or whether antitrust laws should be used to address competition concerns with the collection of data. Do you have an opinion about the best approach to address this issue or should we be looking at a combination of different approaches?**

Meta has long called for regulation in the digital space on issues like privacy and data security, combating foreign election interference, content moderation, and data portability. The issues facing the industry are complex, multi-faceted, and impact peoples' lives. Accordingly, Meta is committed to working with policymakers to craft the right regulations. Meta is amenable to reviewing proposed legislation and providing comments.

More information about our approach to regulation can be found here: https://about.meta.com/regulations/?utm_source=about.facebook.com&utm_medium=redirect.

Senator Josh Hawley
Questions for the Record to Steve Satterfield, Vice President of Privacy & Public Policy, Facebook

1. **Please provide copies of all research findings or reports, whitepapers, slideshows, meeting recordings, or other documentation circulated within Facebook, over the past ten years, pertaining to each of the following topic areas:**

    a) **Addiction or addictive behaviors associated with the use of Facebook's products and services;**
    b) **Depression and/or self-harm associated with the use of Facebook's products and services;**
    c) **Impact of Facebook's products and services on the mental health and wellness of users under age 18;**
    d) **Extent to which Facebook's products and services are accessed by users under age 13**
    e) **Development of novel products or services targeted specifically to users under age 13.**

We want social media to be a positive force in teens' lives, so we're listening to feedback from experts and our community to build apps where teens can discover and create in an age-appropriate way; as part of that work, we have developed tools and features to support keeping young people even safer on Instagram. For example:

> **Parental Tools.** We are committed to working with parents and families, as well as experts in child development, online safety, and children's health and media, to ensure we are building appropriate tools and features for families. That means building tools that promote meaningful interactions and helping people manage their time on our platform. It also means providing information, resources, and tools for parents and teens to work together to develop healthy and safe online habits. And it means continued learning in this area.
>
> We believe that parents and guardians know what is best for their teens, and we've developed more than 30 tools to support teens and families, including developing supervision tools that allow parents and guardians to ask teens to enable them to be more involved in their teens' experiences. In March 2022, we rolled out supervision tools that allow parents and guardians to: (1) view how much time their teens spend on Instagram and set time limits; (2) be notified when their teen shares they've reported someone; and (3) view and receive updates on what accounts their teens follow and the accounts that follow their teens. In June 2022, we introduced additional features that allow parents and guardians to send invitations to their teens to initiate supervision tools, set specific times when they would like to limit their teen's use of Instagram, and see more information when their teen reports an account or post, including who was reported, and the type of report. We make video tutorials on how to use these supervision tools available for parents and guardians in the Family Center's education hub.
>
> Additionally, in November 2022, we introduced updates on Facebook and Instagram to help further protect teens from online harm. For example, everyone who is under the age of 16 (or

under 18 in certain countries) is now defaulted into more private settings when they join Facebook (a change we announced for Instagram in July 2021), and we encourage teens already on the app to choose these more private settings. We are also working with the National Center for Missing and Exploited Children to build a global platform for teens who are worried intimate images they created might be shared on public online platforms without their consent. This platform will be similar to work we have done to prevent the non-consensual sharing of intimate images for adults. It will allow us to help prevent a teen's intimate images from being posted online and can be used by other companies across the tech industry. In addition, we are working with Thorn and their NoFiltr brand to create educational materials that reduce the shame and stigma surrounding intimate images, and empower teens to seek help and take back control if they've shared them or are experiencing sextortion.

Take A Break. We also launched "Take A Break" in certain countries to empower people to make informed decisions about how they're spending their time. If someone has been scrolling for a certain amount of time, we ask them to take a break from Instagram and suggest that they set reminders to take more breaks in the future. We also show them expert-backed tips to help them reflect and reset. To make sure that teens are aware of this feature, we show them notifications suggesting they turn these reminders on.

Nudging Teens Towards Different Topics if They've Been Dwelling on One Topic for a While. Our research shows—and external experts agree—that if people are dwelling on one topic for a while, it could be helpful to nudge them towards other topics at the right moment. That's why we built an experience that will nudge people towards other topics if they've been dwelling on one topic for a while. This nudge is designed to encourage teens to discover something new and excludes certain topics that may be associated with appearance comparison.

We designed this feature because research suggests that nudges can be effective for helping people — especially teens — be more mindful of how they're using social media in the moment. In an external study on the effects of nudges on social media use, 58.2% of respondents agreed or strongly agreed that nudges made their social media experience better by helping them become more mindful of their time on-platform. Our own research shows they're working too: during a one-week testing period, one in five teens who saw our new nudges switched to a different topic.

In addition to this work, we prohibit people under the age of 13 from using Facebook and Instagram, and when we learn that someone under 13 years old is on our platform, we remove them. We also continue to develop ways for people to verify their age on Instagram, allowing us to provide age-appropriate experiences. For example, in June 2022, we began testing new options for people on Instagram to verify their age, starting with people based in the US. If someone attempts to edit their date of birth on Instagram from under the age of 18 to 18 or over, we'll require them to verify their age using options such as uploading their ID or recording a video selfie. We're testing this so we can make sure teens and adults are in the right experience for their age group. We are also partnering with Yoti, a company that specializes in online age verification, to help ensure people's privacy.

Our age verification tests show that our tools are working to help keep people within age-appropriate experiences. Since we began these new tools on Instagram, we've found that approximately four times as many people were more likely to complete our age verification requirements (when attempting to edit their date of birth from under 18 to over 18), equating to hundreds of thousands of people being placed in experiences appropriate for their age. We also were able to stop 96% of the teens who attempted to edit their birthdays from under 18 to 18 or over on Instagram from doing so. And we have found that 81% of people presented with our menu of options chose to use Yoti's video selfie to verify their age.

Meta conducts research on these important issues to understand how people experience its apps. We use our research to inform changes to our apps and provide resources for the people who use them. We are committed to learning even more about issues related to well-being, and we welcome the opportunity to work with Congress and others in the industry on this important topic.

We offer researchers a number of privacy-protective methods to collect and analyze data. We welcome research that challenges us to innovate and that doesn't compromise the security of our platform or the privacy of the people who use it. Meta researchers have also published and shared hundreds of papers, and we will continue to work to publish research externally and to engage and collaborate with experts, including in data-sharing with researchers on issues related to young people. For more information about research we make available, please visit https://research.facebook.com/.

Finally, in December 2022, we held our first Meta Summit focused on Youth Safety and Well-Being to discuss this work. Safety advocates, mental health experts, educators, think tank researchers, policy writers and parents—many of whom helped inform the development of these tools—gathered in Washington, D.C. to discuss challenges families face in the digital age and explore opportunities to better serve teens and families. At the Summit, Nick Clegg, Meta's President of Global Affairs, called for global policymakers and regulators to work together on clear, consistent regulation when it comes to providing safe, age-appropriate experiences for young people online. We support regulators across the globe working together to establish clear, consistent laws that adapt to ever-evolving technologies, so they can be implemented successfully by companies across our industry. We're hopeful that continued regulation in this area will seek to preserve teens' rights to be online, while creating safe, supportive environments for them to express themselves.

2. **Please provide the following information:**

    a) **How much revenue, in the aggregate, does Facebook estimate that it makes from users under 18?**
    b) **How much revenue does Facebook estimate that it makes from *each individual* user under 18?**
    c) **How much revenue, in the aggregate, does Facebook estimate that it makes from users under 13?**
    d) **How much revenue does Facebook estimate that it makes from *each individual* user under 13?**

We publicly report our Average Revenue per User ("ARPU") on Facebook, both for advertising and other revenue, broken out by geographic region. In the US and Canada, Facebook's ARPU from advertising was $58.77 in the fourth quarter of 2022. We also report the Average Revenue per Person ("ARPP") across Meta's family of apps, both for advertising and other revenue. Meta's ARPP from advertising across its family of apps was $8.63 in the fourth quarter of 2022. For more information, please see our latest earnings presentation (https://s21.q4cdn.com/399680738/files/doc_financials/2022/q4/Earnings-Presentation-Q4-2022.pdf). We do not break out this information publicly by age. We prohibit people under the age of 13 from using Facebook and Instagram, and when we learn that someone under 13 years old is on our platform, we remove them.

3. **On September 27, Instagram head Adam Mosseri announced that the company was pausing efforts "to build an Instagram experience for people under the age of 13, often referred to as 'Instagram Kids,'" but "[stood] by the need to develop this experience" and intended "to work with parents, experts, policymakers and regulators, to listen to their concerns, and to demonstrate the value and importance of this project for younger teens online today."**

   a) **When, if at all, does Facebook project that it will resume development on "an Instagram experience for people under the age of 13"?**
   b) **On the basis of what considerations did Facebook conclude that it was more important to develop a designated digital space for users under 13 than, conversely, to ramp up efforts to prevent use of the platform by these users altogether?**

We started work to build an Instagram experience for tweens (aged 10-12) to address an issue seen across our industry: tweens are getting phones younger and younger, misrepresenting their age, and downloading apps that are meant for those 13 or older. This is an industry-wide concern, and other tech companies have built experiences for tweens. For example, YouTube and TikTok both have versions of their apps built specifically for those under 13. Additionally, we launched Messenger Kids in 2017 after meeting with thousands of parents, parenting organizations, child safety advocates and child development experts about the need for a messaging app that lets kids have fun connecting with friends and family while giving parents control over the experience.

The Instagram experience for tweens was intended to focus on delivering age-appropriate experiences and provide parents and guardians visibility and control over what their tweens are doing online. While we stand by the need to develop this Instagram experience, in September 2021, we announced that we were pausing this work. To be clear, our intention was not for this version to be the same as Instagram today. It was never meant for younger kids, but for tweens (aged 10-12). It would have required parental permission to join, we would not have shown ads, and it would have had age-appropriate content and features. Parents would have been able to supervise the time their tweens spent on the app and oversee who could message them, who could follow them, and whom they could follow.

We also continue to build technology to find and remove Instagram accounts belonging to people under the age of 13. We have tools and processes to identify and remove people who falsely state they are 13 years old or older. For example, anyone can report an underage account to us. Our content reviewers are also trained to flag reported accounts that appear to be used by people who are underage. If these people are unable to prove they meet our minimum age requirements, we delete their accounts. In the last two quarters of 2021, Meta removed more than 4.8 million accounts on Facebook and 1.7 million accounts on Instagram because they were unable to meet our minimum age requirement.

Senator Thom Tillis
Questions for the Record to Steve Satterfield, Vice President of Privacy & Public Policy, Facebook

1. **The term "data" can have multiple meanings, which can sometimes generate confusion in policy discussions. How would you define "data" and "big data", as used in your written testimony?**
   a. **How would you define consumer and user data, specifically what would be included and excluded from these definitions?**
   b. **Would this include user uploaded videos, images, and text?**
   c. **Would such content be considered part of the "user" data, even if it includes content that originates from other sources?**
   d. **Does it include data in which intellectual property rights, including copyright, trade secret, trademark, or design rights, may subsist?**

As explained in our Privacy Policy, we collect four basic categories of data about people: (1) data about their activity and information they provide; (2) data about their friends, followers, and other connections; (3) data about their app, browser and devices; and (4) data we receive from partners, vendors and third parties, including the websites and apps that use our business tools. Our Privacy Policy provides more detail about each of the four categories.

People retain ownership of the intellectual property rights (things like copyright or trademarks) in any such content that they create and share on our platforms. Nothing in our Terms of Service takes away the rights people have to their own content, and they are free to share their content with anyone else, wherever they want.

As far as the amount of data we collect about people, the answer depends on the person. People who have only recently signed up for Facebook have usually shared only a few things—such as name, contact information, age, and gender. Over time, as people use our products and interact with our services, we receive more data from them, and this data helps us provide more relevant content and services. That data will fall into the categories noted above, but the specific data we receive will, in large part, depend on how the person chooses to use Facebook. For example, some people use Facebook to share photos, so we receive and store photos for those people. Some people enjoy watching videos on Facebook; when they do, we receive information about the video they watched, and we can use that information to help show other videos in their Feeds. Other people seldom or never watch videos, so we do not receive the same kind of information from them, and their Feeds are likely to feature fewer videos.

The data we have about people also depends on how they have used our controls. For example, people who share photos can easily delete those photos. The same is true of any other kind of content that people post on our services. Through Facebook's Activity Log tool, people can also control information about their engagement—i.e., their likes, shares, and comments— with other people's posts. The use of these controls affects the data we have about people.

We also offer a variety of tools to help users understand the data Facebook has about them. These include the Access Your Information and Download Your Information tools available to people who use Facebook in their account settings. And to provide more transparency and control around these practices, Off-Facebook Activity lets people see a summary of apps and websites that send us information about their activity and allows them to disconnect this information from their account if they choose. For more information about this tool, please see our Help Center.

2. **Ad-revenue used to support online piracy is a longstanding problem. Criminals profit by receiving advertising dollars in exchange for giving users free access to stolen movies, music, books, software, and other materials—stealing money from hardworking creators, including many small businesses and individual artists. A recent report found that over *a billion dollars a year* in advertising goes to supporting online pirated content.[1] Both the US and EU have been working on voluntary "follow the money" initiatives for several years with various actors, including Facebook, to stop funding theft. Yet the same report found that Facebook was a top ad spender, accounting for 27% of major brand advertising appearing on piracy apps.[2] This is particularly alarming given that other digital advertisers "almost never appear on piracy apps."[3]**

    a. **What steps does Facebook take, both in the United States and worldwide, to prohibit advertising on piracy websites and applications?**
    b. **Why was Facebook identified as the top major brands involved in placing advertising on applications? What measures is Facebook taking to change this?**
    c. **Does Facebook agree that supporting commercial-scale pirate websites and apps through advertising dollars is wrong?**
    d. **Does Facebook, or its agents or subsidiaries, identify websites or apps that pose a risk of distributing or displaying copyright protected content without authorization?**
    e. **Does Facebook, or its agents or subsidiaries, restrict the display of its advertisements on websites that infringe copyright, or pose a high risk of engaging in copyright infringement?**
    f. **Does Facebook, or its agents or subsidiaries, block payment for ad impressions on pirated content?**
    g. **Does Facebook, or its agents or subsidiaries, conduct independent audits to ensure that any policies are being implemented effectively? How frequently are policies reviewed?**
    h. **Does Facebook collect data over its own ad placements that would allow it to prevent placement on websites or apps that pose a high risk for distributing illegal content, including pirated content?**
    i. **What steps is Facebook taking to enhance transparency of its activities on its advertising networks?**

[1] Digital Citizens Alliance and White Bullet, *Breaking (B)ads: How Advertiser-Supported Piracy Helps Fuel A Booming Multi-Billion Dollar Illegal Market* (July 2021), https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf.

[2] *Id.,* pg. 17.

[3] *Id.*, pg. 17.

Facebook takes creativity, copyright, and protection of intellectual property rights seriously. We strongly oppose the placement of our advertisements on websites and apps that either infringe or pose a high risk of infringing copyright (including on commercial-scale pirate websites and apps). We maintain a robust framework to combat misplacement of Facebook ads on third-party websites and apps. Part of that work involves taking proactive steps to protect IP and combat piracy and the sale and promotion of counterfeit goods.

Advertisement Fraud Management Framework. The goal of our advertisement fraud management framework is two-fold: (i) to prevent fraudulent traffic sources from bidding on or serving Facebook ads; and (ii) to prevent payments for identified fraud traffic. To accomplish these goals, our general practice is to request third-party agencies with whom we contract to proactively identify and protect against fraudulent traffic.

Our current ad fraud management framework is divided into three activities: (1) prevention; (2) detection; and (3) mitigation:

1. **Prevention:** Fraud prevention begins during advertisement network selection. From this selection process, Facebook contracts with industry-leading third-party digital media agencies to place ads for our platforms and services on external websites and apps. Our general practice is to request direct, transparent placements, and request that fraud terms be included in our agreements. In negotiating these agreements, we generally request that vendors agree to actively monitor ad campaigns for signs of fraudulent activity, and agree to alert us in the event that any such activity is detected or suspected. Our general practice also includes that vendors agree to ensure that our ads do not appear adjacent to any content promoting subjects such as pornography, non-gaming violence, or infringement of intellectual property rights (including music and video piracy) or on websites that promote those activities. While each agreement is unique, the foregoing reflects some of the terms that we strive to obtain in our agreements with vendors.

2. **Detection:** We utilize tools and fraud suites from third-party agencies, such as the Kochava Fraud Console and tools from Forensiq and DoubleVerify, to try to detect fraudulent placements (including advertisements on websites that either infringe or pose a high risk of infringing copyright). We monitor these placements and try to identify any anomalies that may signal fraudulent or suspicious activity. We, in close collaboration with these third-party agencies, also develop custom, threshold-based signals to detect app and web traffic that leads to suspicious activity.

3. **Mitigation:** We maintain global blocklists intended to prevent our ads from appearing on apps and websites associated with fraud, fake actors, or sensitive content. Our partnership with third-party agencies allows us to permanently block identified fraudulent ad sources, such as websites and apps, and to identify potentially problematic traffic, which is flagged for investigation in partnership with the ad network/publisher. Since our November 2021 response to you on this topic, we have doubled down on the breadth of these efforts. We are now also working with industry stakeholders across the world to identify websites that may be dedicated to piracy or to facilitating copyright infringement. Once identified via our trusted sources, we use internal criteria to identify which URLs should be added to our

blocklists. Meta ads will not appear on any external URL that has been added to the blocklist—thereby significantly reducing any risk of funding or facilitating piracy on the Facebook platform. Further, our mitigation framework consists of utilizing automatic and manual blocking technology to investigate problematic traffic with ad networks. Finally, if any fraud or violations of the underlying agreement with the ad placement agency are identified, our practice is to request refunds for the ad impression. We recognize that no matter our preventative measures, there must always be ongoing manual traffic reviews to spot and investigate suspicious signals. As such, we regularly assess and continue to make improvements to our detection and protection framework, to improve our detection of ads that appear on or are attributed to fraud traffic sources.

Through partnership with third-party agencies, we strive to update our blocklists weekly. Additionally, these third-party agencies have advised us that they conduct regular audits (on the weekly and monthly level) to evaluate fraud safety measures. Managing our ad placements globally can be challenging and is an iterative process. For example, for one of the ads referenced in the Breaking (B)ads report, our teams determined that ten versions or variations of the piracy app already appeared on our permanent blocklist. Further, as a result of the information provided in the report, our teams added an additional four variations of the app to our permanent blocklist. As detailed above, we, in close partnership with third-party vendors, continue to proactively identify how we can improve in this area, and take steps to help protect current and non-users from seeing ads on inappropriate websites and apps, including on those that either infringe or pose a high risk of infringing copyright advertisements.

3. **Your written testimony states that there are "always risks when people transfer data online." Please elaborate on the nature and scope of these risks, and the people and entities who are implicated by these risks.**

   a. **What steps does Facebook take to inform others of these risks?**

Last year, we rewrote and re-designed our Privacy Policy to make it easier to understand and clearer about how we use people's information, and we updated our Terms of Service to better explain what is expected from us and those who use our platforms. The updates to our Privacy Policy include detailed explanations about how we use and share information with third parties. Also, our Help Center contains information and answers to frequently asked questions. When a user decides to login with Facebook or connect their account, we provide information about where they are sending the data, what that destination will receive, and access to that destination's privacy policy.

   b. **How does the Data Transfer Project address these risks?**

The open source Data Transfer Project is a collaborative effort by a group of companies, including Meta, to build a common framework with open-source code that can connect any two online services, enabling a seamless user-initiated portability of data between platforms. The Data Transfer Project's open-source framework powers our Transfer Your Information tool, which enables people to transfer their Facebook photos and videos, notes, posts, and events directly to destinations including BackBlaze, Dropbox, Koofr, Google Photos, Photobucket, Google Calendar, Google Docs, Blogger, and WordPress.

In 2018, the Data Transfer Project published a white paper describing the fundamentals of the project and its principles on a range of topics including privacy and security.

Neither the Data Transfer Project, nor any one company acting alone can resolve the challenging tradeoffs involving data portability like those we identified in our own 2019 white paper on data portability.

4. **Ms. Slaiman advocates for "a digital regulator to comprehensively the policy questions surrounding digital platforms."**
    a. **Do you agree that this is necessary?**
    b. **Given the many issues beyond privacy and competition that address and implicate digital policy—including cybersecurity, national security, consumer rights, free speech, and intellectual property concerns—what existing agency would be the best situated, in your view, to carry out this role?**
    c. **Is it important to you that the regulator should be politically accountable?**

We support updated regulations in the digital space on issues like privacy and data security, combating foreign election interference, content moderation, and data portability, and we have called for the US to create a new digital regulator. The issues facing the industry are complex, multi-faceted, and impact peoples' lives. Accordingly, Meta is committed to working with policymakers to craft the right regulations, and is amenable to reviewing proposed legislation and providing comments.

We have been open about our support for updated regulations on key issues. More information about our approach to regulation can be found here: https://about.meta.com/regulations/?utm_source=about.facebook.com&utm_medium=redirect.