A Look Behind the Screens

Examining the Data Practices of Social Media and Video Streaming Services

Federal Trade Commission
September 2024

A Look Behind the Screens

Examining the Data Practices of Social Media and Video Streaming Services

An FTC Staff Report

September 2024

FEDERAL TRADE COMMISSION

Contents

Preface

by Samuel Levine
Director, Bureau of Consumer Protection

In December 2020, the Federal Trade Commission issued 6(b) Orders to nine of the largest social media and video streaming services—Amazon, Facebook, YouTube, Twitter, Snap, ByteDance, Discord, Reddit, and WhatsApp ("Companies"). At the time, a bipartisan group of Commissioners issued a joint statement warning that far too much about how these platforms operate is "dangerously opaque," with critical questions around data collection and algorithms "shrouded in secrecy."[1] "It is alarming," the statement notes, "that we still know so little about companies that know so much about us."[2]

Today, the Commission is approving the release of a groundbreaking report that sheds light on how these powerful Companies have operated. It shows how the tech industry's monetization of personal data has created a market for commercial surveillance, especially via social media and video streaming services, with inadequate guardrails to protect consumers. The report finds that these Companies engaged in mass data collection of their users and – in some cases – non-users. It reveals that many Companies failed to implement adequate safeguards against privacy risks. It sheds light on how Companies used our personal data, from serving hyper-granular targeted advertisements to powering algorithms that shape the content we see, often with the goal of keeping us hooked on using the service. And it finds that these practices pose unique risks to children and teens, with the Companies having done little to respond effectively to the documented concerns that policymakers, psychologists, and parents have expressed over young people's physical and mental wellbeing.

Staff's report includes detailed analysis of each of these issues and more, and it offers recommendations on how to address these risks. In my view, this report – and the process of putting it together – should point policymakers to three key takeaways.

The Status Quo Is Unacceptable: The amount of data collected by large tech companies is simply staggering. They track what we read, what websites we visit, whether we are married and have children, our educational level and income bracket, our location, our purchasing habits, our personal interests, and in some cases even our health conditions and religious faith. They track what we do on *and off* their platforms, often combining their own information with enormous data sets purchased through the largely unregulated consumer data market. And large firms are increasingly relying on hidden pixels and similar technologies – embedded on other websites – to track our behavior down to each click. In fact, the Companies collected so much data that in response to the Commission's

---

[1] Rohit Chopra, Rebecca Kelly Slaughter & Christine S. Wilson, FED. TRADE COMM'N, Joint Statement Regarding Social Media and Video Streaming Service Providers' Privacy Practices, (Dec. 14, 2020), https://www.ftc.gov/system/files/documents/public_statements/1584150/joint_statement_of_ftc_commissioners_chopra_slaughter_and_wilson_regarding_social_media_and_video.pdf.

[2] *Id.*

questions, they often could not even identify all the data points they collected or all of the third parties they shared that data with.

The report leaves no doubt that without significant action, the commercial surveillance ecosystem will only get worse. Our privacy cannot be the price we pay to accomplish ordinary basic daily activities, and responsible data practices should not put a business at a competitive disadvantage.

Self-Regulation Is Not the Answer: Despite widespread support for federal privacy standards, Congress has yet to pass comprehensive legislation on privacy, algorithmic accountability, or teen online safety. The absence of legislation has given firms nearly free rein in how much they can collect from users. Two decades ago, some believed that large tech companies could be trusted to establish adequate privacy standards and practices. This report makes clear that self-regulation has been a failure. Predicting, shaping, and monetizing human behavior through commercial surveillance is extremely profitable – it's made these companies some of the most valuable on the planet – and putting industry in charge has had predictable results. America's hands-off approach has produced an enormous ecosystem of data extraction and targeting that takes place largely out of view to consumers. While there have been isolated instances of firms taking pro-privacy actions, those continue to be the exceptions that prove the rule. We've seen over and over that, when the financial interest in extracting personal information collides with the interest in protecting consumer privacy, consumers lose out.

As many of these firms pivot to developing and deploying AI, while continuing to shroud their practices in secrecy and implementing minimal safeguards to protect users, we must not continue to let the foxes guard the henhouse. Protecting users – especially children and teens – requires clear baseline protections that apply across the board.

To Fix the System, Fix the Incentives: Staff's report includes detailed findings around a host of issues ranging from indiscriminate data collection to hyper-granular targeting, each of which should concern policymakers. But these findings should not be viewed in isolation. They stem from a business model that varies little across these nine firms – harvesting data for targeted advertising, algorithm design, and sales to third parties. With few meaningful guardrails, companies are incentivized to develop ever-more invasive methods of collection.

This incentive structure is especially concerning given the dominant positioning enjoyed by the largest firms, which exert vast power over our economy, our democracy, and our society. The rewards from data harvesting raise serious risks that firms will seek unfair advantages through a host of anti-competitive behaviors – from pressuring smaller websites to embed their tracking technologies, to leveraging their massive collection efforts to identify and prevent newcomers who want to enter the market, to creating vast 'walled gardens' that do much to depress competition and little to protect consumers' data.

As policymakers consider different approaches to protecting the public, focusing on the root causes of many harms – and not just the symptoms – is key.

* * *

I want to conclude by thanking our staff for their diligence and persistence, particularly given the lack of cooperation from many of the 6(b) Order recipients. Echoing the way that firms conceal and hide their collection practices, many of the Companies provided the Commission with limited,

incomplete, or unhelpful responses that appeared to have been carefully crafted to be self-serving and avoid revealing key pieces of information.[3] Ultimately, the Commission – backed with the threat of taking these firms to court to enforce the FTC's 6(b) Orders – was able to gather enough information to address the key concerns that led the agency to issue this study. The result is that the public now has much more insight – and much to be alarmed about – with respect to the commercial surveillance ecosystem.

[3] For example, staff's requests for a comprehensive list of data points that the Companies collected were often met with stonewalling, foot-dragging, and partial responses that concealed the full scope of their collection efforts.

Executive Summary

Social Media and Video Streaming Services ("SMVSSs")[4] have become a ubiquitous part of our daily lives and culture. Various types of SMVSSs provide places where people can connect, create, share, or stream everything from media content like videos, music, photos, and games; comment on or react to content; connect with and send messages to other users; join, participate in, or subscribe to groups, message boards, or content channels; read or watch news; and consume advertisements for consumer products. Unsurprisingly, this ease of accessing information and connecting others has transformed our society in many ways.

These types of services let you connect with the world from the palm of your hand. At the same time, many of these services have been at the forefront of building the infrastructure for mass commercial surveillance. Some firms have unique access to information about our likes and dislikes, our relationships, our religious faiths, our medical conditions, and every other facet of our behavior, at all times and across multiple devices. This vast surveillance has come with serious costs to our privacy. It also has harmed our competitive landscape and affected the way we communicate and our well-being, especially the well-being of children and teens. Moreover, certain large SMVSSs may enjoy significant market power and therefore face fewer competitive constraints on their privacy practices and other dimensions of quality.

In December 2020, the Federal Trade Commission ("Commission" or "FTC") issued identical Orders to File Special Reports under Section 6(b) of the FTC Act to a cross-section of nine companies in the United States in order to gain a better understanding of how their SMVSSs affect American consumers.[5] Appendix A to this report (hereinafter "Appendix A") is a copy of the text of the Order that the Commission issued to these nine Companies.[6]

This report is a culmination of that effort. Based on the information provided in response to the Commission's Orders, publicly available materials, and the Commission's long experience with SMVSSs, this report highlights the practices of the Companies' SMVSSs, which include social networking, messaging, or video streaming services, or photo, video, or other content sharing applications available as mobile applications or websites. The report contains five sections relating to

---

[4] The Order defines Social Media and Video Streaming Service as "any product or service that allows users to create and share content with other users (whether a private or group interaction) through an application or website on any device (e.g., personal computer, iOS device, Android device, etc.), or stream video, Including, but not limited to, any social networking service, messaging service, video streaming service, or photo, video, or other content sharing application, whether offered for a fee or for free." FED. TRADE COMM'N, 6(B) SMVSS STUDY SAMPLE ORDER (2020), Definition II, https://www.ftc.gov/system/files/documents/reports/6b-orders-file-special-reports-social-media-service-providers/6bs_order_os_final.pdf.

[5] Press Release, Fed. Trade Comm'n, FTC Issues Orders to Nine Social Media and Video Streaming Services Seeking Data About How They Collect, Use, and Present Information (Dec. 14, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/12/ftc-issues-orders-nine-social-media-video-streaming-services-seeking-data-about-how-they-collect-use.

[6] *See also* FED. TRADE COMM'N, 6(B) SMVSS STUDY SAMPLE ORDER (2020), https://www.ftc.gov/system/files/documents/reports/6b-orders-file-special-reports-social-media-service-providers/6bs_order_os_final.pdf .

the following topics: (1) data practices, such as collection, use, disclosure, minimization, retention, and deletion; (2) advertising and targeted advertising; (3) the use of automated decision-making technologies; (4) practices relating to children and teens; and (5) concerns relating to competition.

1. Summary of Key Findings

This report makes the following general findings, although each finding may not be applicable to every one of the Companies in every instance:

- **Many Companies collected and could indefinitely retain troves of data from and about users and non-users, and they did so in ways consumers might not expect.** This included information about activities both on and off of the SMVSSs, and included things such as personal information, demographic information, interests, behaviors, and activities elsewhere on the Internet. The collection included information input by users themselves, information gathered passively or inferred, and information that some Companies purchased about users from data brokers and others, including data relating to things such as household income, location, and interests. Moreover, many Companies' data practices posed risks to users' and non-users' data privacy, and their data collection, minimization, and retention practices were woefully inadequate. For instance, minimization policies were often vague or undocumented, and many Companies lacked written retention or deletion policies. Some of the Companies' SMVSSs did not delete data in response to user requests—they just de-identified it. Even those Companies that actually deleted data would only delete some data, but not all.

- **Many Companies relied on selling advertising services to other businesses based largely on using the personal information of their users. The technology powering this ecosystem took place behind the scenes and out of view to consumers, posing significant privacy risks**. For instance, some Companies made available privacy-invasive tracking technologies such as pixels, which have the ability to transmit sensitive information about users' actions to the SMVSSs that use them. Because the advertising ecosystem is complex and occurs beneath the surface, it is challenging for users to decipher how the information collected from and about them is used for ad targeting—in fact, many users may not be aware of this at all. Some Companies' ad targeting practices based on sensitive categories also raise serious privacy concerns.

- **There was a widespread application of Algorithms, Data Analytics,[7] or artificial intelligence ("AI"),[8] to users' and non-users' personal information. These technologies**

[7] The Order defines "Algorithms or Data Analytics" as "the process of examining and analyzing data in order to find patterns and make conclusions about that data, whether by machine or human analyst." Appendix A, Definition E. *See also* Section VI for more information regarding the Companies' use of Algorithms, Data Analytics, or AI.

[8] AI is an ambiguous term with many possible definitions, but it "often refers to a variety of technological tools and techniques that use computation to perform tasks such as predictions, decisions, or recommendations." Michael Atleson, *Keep your AI claims in check*, FED. TRADE COMM'N (Feb. 27, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check. Machine learning, natural language processing, and other tools are usually considered branches, types, or applications of AI. FED. TRADE COMM'N, COMBATTING ONLINE HARMS THROUGH

powered the SMVSSs—everything from content recommendation to search, advertising, and inferring personal details about users. Users lacked any meaningful control over how personal information was used for AI-fueled systems. This was especially true for personal information that these systems infer, that was purchased from third parties, or that was derived from users' and non-users' activities off of the platform. This also held true for non-users who did not have an account and who may have never used the relevant service. Nor were users and non-users empowered to review the information used by these systems or their outcomes, to correct incorrect data or determinations, or to understand how decisions were made, raising the potential of further harms when systems may be unreliable or infer sensitive information about individuals. Overall, there was a lack of access, choice, control, transparency, explainability, and interpretability relating to the Companies' use of automated systems. There also were differing, inconsistent, and inadequate approaches relating to monitoring and testing the use of automated systems. Other harms noted included Algorithms that may prioritize certain forms of harmful content, such as dangerous online challenges, and negative mental health consequences for children and teens.

- **The trend among the Companies was that they failed to adequately protect children and teens—this was especially true of teens, who are not covered by the Children's Online Privacy Protection Rule ("COPPA Rule").**[9] Many Companies said they protected children by complying with the COPPA Rule but did not go further. Moreover, in an apparent attempt to avoid liability under the COPPA Rule, most SMVSSs asserted that there are no child users on their platforms because children cannot create accounts. Yet we know that children are using SMVSSs. The SMVSSs should not ignore this reality. When it comes to teens, SMVSSs often treat them as if they were traditional adult users. Almost all of the Companies allowed teens on their SMVSSs and placed no restrictions on their accounts, and collected personal information from teens just like they do from adults.

The past can teach powerful lessons. By snapshotting the Companies' practices at a recent moment in time (specifically, the Orders focused on the period of 2019–2020) and highlighting the implications and potential consequences that flowed from those practices, this report seeks to be a resource and key reference point for policymakers and the public.

2. Summary of Competition Implications

- **Data abuses can fuel market dominance, and market dominance can, in turn, further enable data abuses and practices that harm consumers.** In digital markets, acquiring and maintaining access to significant user data can be a path to achieving market dominance and building competitive moats that lock out rivals and create barriers to market entry. The competitive value of user data can incentivize firms to prioritize acquiring it, even at the expense

---

INNOVATIONS (June 16, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf. *See infra* Section VI for more information on Algorithms, Data Analytics, or AI.

[9] 16 C.F.R. pt. 312.

of user privacy. Moreover, a company's practices with respect to privacy, data collection, data use, and automated systems can comprise an important part of the quality of the company's product offering. A lack of competition in the marketplace can mean that users lack real choice among services and must surrender to the data practices of a dominant company, and that companies do not have to compete over these dimensions—depriving consumers of additional choice and autonomy. In sum, limited competition can exacerbate the consumers harms described in this report.

3. Summary of Staff Recommendations

- **Companies can and should do more to protect consumers' privacy, and Congress should enact comprehensive federal privacy legislation that limits surveillance and grants consumers data rights.** Baseline protections that Companies should implement include minimizing data collection to only that data which is necessary for their services and implementing concrete data retention and data deletion policies; limiting data sharing with affiliates, other company-branded entities, and third parties; and adopting clear, transparent, and consumer-friendly privacy policies.

- **Companies should implement more safeguards when it comes to advertising, especially surrounding the receipt or use of sensitive personal information**. Baseline safeguards that Companies should implement include preventing the receipt, use, and onward disclosure of sensitive data that can be made available for use by advertisers for targeted ad campaigns.

- **Companies should put users in control of—and be transparent about—the data that powers automated decision-making systems, and should implement more robust safeguards that protect users.** Changing this would require addressing the lack of access, choice, control, transparency, explainability, and interpretability relating to their use of automated systems; and implementing more stringent testing and monitoring standards.[10]

- **Companies should implement policies that would ensure greater protection of children and teens.** This would include, for instance, treating the COPPA Rule as representing the minimum requirements and providing additional safety measures for children as appropriate; recognizing that teen users are not adult users and, by default, afford them more protections as they continue to navigate the digital world; providing parents/legal guardians a uniform, easy, and straightforward way to access and delete their child's personal information.

- **Firms must compete on the merits to avoid running afoul of the antitrust laws**. Given the serious consumer harms risked by lackluster competition, antitrust enforcers must carefully scrutinize potential anticompetitive acquisitions and conduct and must be vigilant to anticompetitive harms that may manifest in non-price terms like diminished privacy.

Staff's full recommendations are at the end of this report.

[10] This report and its recommendations do not address or endorse any attempt to censor or moderate content based on political views.

I. Introduction

The growth of social media over a short span of time has been nothing short of astounding. From 2005 to 2019, the percentage of adults in the United States who used social media increased from 5% to 79%; by 2019, many social media platforms had billions of monthly active users worldwide, and an estimated one in three people worldwide were using social media.[11] It is no exaggeration to state that social media has transformed major facets of consumers' lives, affecting how they communicate, consume news, and interact with products and services. At a macro level, the effects of social media are just as profound, shaping everything from elections to public health to matters of war and peace.

As social media has extended into nearly every aspect of society, the data practices of social media companies demand attention and scrutiny. The rise of social media correlates closely with the amount of time people are spending online. Adults in the United States spend on average more than six hours daily on digital media (i.e., apps and websites accessed through mobile phones, tablets, computers, and other connected devices such as game consoles).[12] As more consumers spend time online and spend increasing amounts of that online time interacting with social media services, the opportunities abound for social media companies to collect more and more data about the actions, behaviors, and preferences of consumers, including details as minute as what you clicked on with your mouse. Since greater "User Engagement" means greater opportunities for monetization through advertising,[13] many also have designed and relied on Algorithms that work to prioritize showing content that fuels the most User Engagement more than anything else, thereby giving them opportunities to keep users online and to collect more information. As a result, social media companies have become repositories of consumer data collected from a variety of sources and have achieved their goal of monetizing this data by creating and selling powerful targeted advertising technologies.

It is against this backdrop that the Commission conducted a comprehensive examination of the practices, as reported, of the Companies and their respective SMVSSs. While the report is thorough and offers key findings and recommendations, this report reflects only a snapshot in time for several reasons:[14]

---

[11] Esteban Ortiz-Ospina, *The Rise of Social Media*, OUR WORLD IN DATA (Sept. 18, 2019), https://ourworldindata.org/rise-of-social-media.

[12] *Id.*

[13] The Order defines "User Engagement" as "how a user, on and off the Social Media and Video Streaming Service, interacts with any product or service of the Social Media and Video Streaming Service (Including, but not limited to, how frequently, for how long, and in what manner)." Appendix A, Definition MM.

[14] Due to Sections 6(f) and 21(d)(1)(B) of the FTC Act prohibiting the Commission from disclosing trade secrets or commercial or financial information that is privileged or confidential, the observations and findings discussed in this report are provided on an anonymous and aggregated basis. *See* 15 U.S.C. §§ 46(f), 57b-2(d)(1)(B).

- **The Applicable Time Period is limited in scope.**[15] The Orders were issued December 14, 2020, and the Companies' responses reflect their practices between January 1, 2019, and December 31, 2020 ("Applicable Time Period"). Thus, this report's findings are based on the Companies' practices from this discrete period in time.[16]

- **Changes in technology.**[17] Technology evolves rapidly, and such changes have affected the topics studied herein to varying degrees. The report endeavors to acknowledge known changes, but it cannot address all technological changes, particularly those known only to a Company.

- **New SMVSSs have emerged, and Companies have changed.**[18] This report does not, and cannot, reflect on the practices of SMVSSs that have been introduced after the Order was issued; nor does it reflect subsequent changes in the Companies' corporate structures or their business models.

- **Changes in use of SMVSSs.** The Orders were issued in 2020, and this report focuses on practices that occurred both immediately prior to and at the height of the COVID-19 pandemic, a unique period in which consumers' engagement over social media evolved and increased.[19]

---

[15] For example, since the Orders were issued in December 2020, Twitter changed ownership. *See infra* Section III for background information on the Companies. Since this ownership change, Twitter is now called "X" and has announced new business practices. *See, e.g.*, Anirudh Saligrama, *Musk says Twitter will limit how many tweets users can read*, REUTERS (July 1, 2023), https://www.reuters.com/technology/musk-says-twitter-applies-temporary-limit-address-data-scraping-system-2023-07-01/.

[16] For this reason, many findings in this report are stated in the past tense. The use of the past tense is not meant to suggest that a Company or SMVSS has stopped a particular practice.

[17] *See, e.g.*, Kate O'Flaherty, *iOS 14.5 Is Available Now With This Powerful New Privacy Feature*, FORBES (Apr. 26, 2021), https://www.forbes.com/sites/kateoflahertyuk/2021/04/26/ios-145-is-available-now-with-this-stunning-new-privacy-feature/?sh=531478b727c4 (discussing update to iOS operating system requiring that users explicitly opt in to being tracked on Apple devices across applications and websites).

[18] *See, e.g.*, Mike Isaac, *Threads, Instagram's 'Twitter Killer,' Has Arrived*, N.Y. TIMES (July 5, 2023), https://www.nytimes.com/2023/07/05/technology/threads-app-meta-twitter-killer.html.

[19] *See* Ella Koeze & Nathaniel Popper, *The Virus Changed the Way We Internet*, N.Y. TIMES (Apr. 7, 2020), https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html.

- **FTC[20] and other regulatory action.[21]** Several Companies were the subject of privacy-related enforcement matters, both domestically and abroad, which resulted in changes to the Companies' privacy practices.[22]

---

[20] *See, e.g.*, *Fed. Trade Comm'n v. Ring LLC*, No. 1:23-cv-01549 (D.D.C. May 31, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023113-ring-llc; *United States v. Amazon.com, Inc.*, No. 2:23-cv-00811 (W.D. Wash. May 31, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3128-amazoncom-alexa-us-v; Facebook, Inc., No. C-4365 (F.T.C. May 3, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter; *United States v. Twitter, Inc.*, No. 3:22-cv-03070 (N.D. Cal. May 25, 2022), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023062-twitter-inc-us-v; *Fed. Trade Comm'n v. Google LLC*, No. 1:19-cv-02642 (D.D.C. Sept. 4, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3083-google-llc-youtube-llc.

[21] Several General Data Protection Regulation ("GDPR") enforcement matters have been brought against Companies or their SMVSSs. *See, e.g.,* Press Release, Data Prot. Comm'n Ir., Data Protection Commission announces conclusion of inquiry into Meta Ireland (May 22, 2023), https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland; Press Release, U.K. Info. Comm'r's Office, ICO fines TikTok £12.7 million for misusing children's data (Apr. 4, 2023), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data/; Press Release, Data Prot. Comm'n Ir., Data Protection Commission announces conclusion of inquiry into WhatsApp (Jan. 19, 2023), https://dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-inquiry-whatsapp; Press Release, Data Prot. Comm'n Ir., Data Protection Commission announces conclusion of two inquiries into Meta Ireland (Jan. 4, 2023), https://dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland; Press Release, Data Prot. Comm'n, Data Protection Commission announces decision in Facebook "Data Scraping" Inquiry (Nov. 28, 2022), https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry; Press Release, Commission Nationale de l'Informatique et des Libertés, DISCORD INC. fined 800 000 euros (Nov. 17, 2022), https://www.cnil.fr/en/discord-inc-fined-800-000-euros; Press Release, Data Prot. Comm'n Ir., Data Protection Commission announces decision in Instagram Inquiry (Sept. 15, 2022), https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry; Press Release, Agencia Española Protección Datos, The AEPD has imposed a sanction on Google LLC for transferring personal data to third parties unlawfully and for hindering the exercise of the right to erasure (May 18, 2022), https://www.aepd.es/en/prensa-y-comunicacion/notas-de-prensa/the-aepd-has-imposed-sanction-on-google-llc-for-transferring-personal-data-to-third-parties; Press Release, Data Prot. Comm'n Ir., Data Protection Commission announces decision in Meta (Facebook) inquiry (Mar. 15, 2022), https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-meta-facebook-inquiry; Press Release, Commission Nationale de l'Informatique et des Libertés, FACEBOOK IRELAND LIMITED fined 60 million euros (Jan. 6, 2022), https://www.cnil.fr/en/cookies-facebook-ireland-limited-fined-60-million-euros; Press Release, Commission Nationale de l'Informatique et des Libertés, Cookies: GOOGLE fined 150 million euros (Jan. 6, 2022), https://www.cnil.fr/en/cookies-google-fined-150-million-euros; Press Release, Data Prot. Comm'n, Data Protection Commission announces decision in WhatsApp inquiry (Sept. 2, 2021), https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry; Sam Shead, *Amazon hit with $887 million fine by European privacy watchdog*, CNBC (July 30, 2021), https://www.cnbc.com/2021/07/30/amazon-hit-with-fine-by-eu-privacy-watchdog-.html; *Dutch data protection authority fines TikTok €750,000 over privacy flaw*, EURONEWS (July 22, 2021), https://www.euronews.com/next/2021/07/22/dutch-data-protection-authority-fines-tiktok-750-000-over-privacy-flaw; Press Release, Data Prot. Comm'n Ir., Data Protection Commission announces decision in Twitter inquiry (Dec. 15, 2020), https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-twitter-inquiry; Press Release, Eur. Data Prot. Bd., Belgian DPA imposes €600.000 fine on Google Belgium for not respecting the right to be forgotten of a Belgian citizen, and for lack of transparency in its request form to delist (July 16, 2020), https://edpb.europa.eu/news/national-news/2020/belgian-dpa-imposes-eu600000-fine-google-belgium-not-respecting-right-be_en; Press Release, Eur. Data Prot. Bd. The Swedish Data Protection Authority imposes administrative fine on Google (Mar. 11, 2020), https://edpb.europa.eu/news/national-news/2020/swedish-data-protection-authority-imposes-administrative-fine-google_en; Press Release, Eur. Data Prot. Bd., The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC (Jan. 21, 2019),

II. Legal Framework Applicable to Social Media and Video Streaming Services

The FTC enforces several laws that apply to SMVSSs (including those that were not Order recipients) and the practices at issue in this report. First, Section 5 of the FTC Act protects consumers through its prohibition on unfair or deceptive practices in or affecting commerce.[23] A misrepresentation or omission is deceptive if it is material and is likely to mislead consumers acting reasonably under the circumstances.[24] An act or practice is unfair if it causes, or is likely to cause, substantial injury that is not reasonably avoidable by consumers, and not outweighed by countervailing benefits to consumers or competition.[25]

For example, Section 5 prohibits companies from making false or misleading statements about their privacy or data security practices, such as misrepresentations about how they collect, use, share, and secure consumers' personal information.[26] Section 5 also prohibits unfair practices that are likely to harm, or do harm, consumers. Unfair data practices include: selling consumers' sensitive location data, including to profile, surveil, and target consumers for advertising purposes;[27] collecting, using, and sharing consumers' sensitive personal information without their knowledge or consent;[28] making retroactive changes to data privacy or security practices or policies, without notifying and obtaining

---

https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en; Press Release, Eur. Data Prot. Bd., Hamburg Data Protection Commissioner's €51,000 fine against Facebook Germany GmbH (Dec. 1, 2019), https://edpb.europa.eu/news/national-news/2019/hamburg-data-protection-commissioners-eu51000-fine-against-facebook-germany_en.

[22] *See also* Clothilde Goujard & Alfred Ng, *EU and US reach a deal to let data flow across the Atlantic*, POLITICO (July 10, 2023), https://www.politico.eu/article/eu-signs-off-on-data-transfers-deal-with-us/ (discussing the European Union's approval of the EU-U.S. Data Privacy Framework, an agreement which allows for transatlantic data exchanges).

[23] 15 U.S.C. § 45(a)(1).

[24] FTC Policy Statement on Deception, 103 F.T.C. 110, 174 (1984) (appended to Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984)), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

[25] 15 U.S.C. § 45(n).

[26] *See, e.g., 1Health.io Inc.*, No. C-4798 (F.T.C. Sept. 7, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923170-1healthiovitagene-matter; *Ring LLC*; Chegg, Inc., No. C-4782 (F.T.C. Jan. 26, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/chegg.

[27] *See, e.g., X-Mode Social, Inc.*, No. C-4802 (F.T.C. Apr. 11, 2024), https://www.ftc.gov/legal-library/browse/cases-proceedings/2123038-x-mode-social-inc.

[28] *See, e.g.*, *United States v. GoodRx Holdings, Inc.,* No. 23–cv–460 (N.D. Cal. Feb. 1, 2023), https://www.ftc.gov/ legal-library/ browse/ cases-proceedings/ 2023090-goodrx-holdings-inc.

consent;[29] or failing to implement measures to prevent the unauthorized disclosure of information.[30] In addition, companies may violate the FTC Act by using automated tools without taking reasonable measures to prevent harm to consumers, such as discriminatorily and inaccurately tagging them as security threats, making claims about AI that are not substantiated, or deploying AI before taking steps to assess and mitigate risks.[31] The FTC has used its enforcement authority to address deceptive and unfair data practices in a myriad of actions relating to privacy and data security, including several Companies that are the subject of this report. For instance, in 2020, the FTC finalized a settlement resolving claims relating to Facebook's alleged violations of a 2012 FTC Order.[32] In 2023, the FTC proposed changes to this 2020 privacy order with Facebook after alleging that the company has failed to fully comply with it, misled parents about their ability to control with whom their children communicated through its Messenger Kids app, and misrepresented the access it provided some app developers to private user data.[33] In 2022, the FTC took action against Twitter, Inc., for deceptively using account security data for targeted advertising, resulting in a $150 million penalty and a permanent injunction.[34]

Second, Section 5 also protects competition by prohibiting unfair methods of competition in or affecting commerce. The FTC's enforcement actions have surfaced how market power can undermine user privacy, and how amassing data—even when it violates people's privacy—can enable firms to build market power. For example, in its lawsuit challenging Facebook's acquisitions of Instagram and WhatsApp as unlawful monopolization, the FTC has argued that users suffered degraded privacy as a result of this illegal conduct.[35]

---

[29] *See, e.g.*, *1Health.io Inc.*

[30] *See, e.g.*, *Ring LLC*.

[31] For example, the FTC has alleged it is an unfair practice to use and deploy AI without taking reasonable steps to address or mitigate risks to consumers, such as by failing to take reasonable steps to regularly track, monitor, test, or assess accuracy. *See Fed. Trade Comm'n v. Rite Aid Corp.*, No. 23-cv-5023 (E.D. Pa. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v. The FTC has also required firms to destroy Algorithms or other work product that were trained on data that should not have been collected. *See, e.g., Ring LLC*; *Everalbum, Inc.*, No. C-4743 (F.T.C. May 5, 2022), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3172-everalbum-inc-matter*; see* Section VI for more information on Algorithms, Data Analytics, or AI.

[32] Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

[33] Press Release, Fed. Trade Comm'n, FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data (May 3, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-blanket-prohibition-preventing-facebook-monetizing-youth-data.

[34] Press Release, Fed. Trade Comm'n, FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads (May 25, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

[35] Press Release, Fed. Trade Comm'n, FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate (Aug. 19, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush-competition-after-string-failed.

Third, the FTC enforces the COPPA Rule,[36] which applies to operators of commercial websites and online services directed to children[37] (including mobile apps and Internet of Things ("IoT") devices) that collect, use, or disclose personal information from children.[38] It also applies to operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from a child, and to websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children.[39] Before an operator covered by the COPPA Rule collects personal information from children, it must provide direct notice to parents[40] and obtain verifiable parental consent.[41] The COPPA Rule also requires that operators must: post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children;[42] provide parents access to their child's personal information to review or have the information deleted;[43] give parents the opportunity to prevent further use or online collection of a child's personal information;[44] maintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security;[45] retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use;[46] and not condition a child's participation in an online activity on the child providing more information than is reasonably necessary to participate in that

---

[36] 16 C.F.R. 312. Congress enacted the Children's Online Privacy Protection Act ("COPPA") in 1998. 15 U.S.C. §§ 6501–6506 (2018). COPPA directed the FTC to promulgate a rule implementing COPPA. The FTC promulgated the COPPA Rule on November 3, 1999, under Section 1303(b) of COPPA, 15 U.S.C. § 6502(b), and Section 553 of the Administrative Procedure Act, 5 U.S.C. § 553. The COPPA Rule went into effect on April 21, 2000. The FTC promulgated revisions to the COPPA Rule that went into effect on July 1, 2013. Pursuant to Section 1303(c) of COPPA, 15 U.S.C. § 6502(c), and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the COPPA Rule constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

[37] The COPPA Rule defines Child as "an individual under the age of 13." *See* 16 C.F.R. § 312.2.

[38] 16 C.F.R. § 312.3.

[39] 16 C.F.R. §§ 312.2 (definition of "Operator"), 312.3. *See generally Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

[40] 16 C.F.R. § 312.4(b).

[41] 16 C.F.R. § 312.5.

[42] 16 C.F.R. § 312.4(d).

[43] 16 C.F.R. § 312.6.

[44] *Id.*

[45] 16 C.F.R. § 312.8.

[46] 16 C.F.R. § 312.10.

activity.[47] The FTC has enforced the COPPA Rule in numerous, varied actions, including against several of the Companies that are the subject of this report.[48] The FTC also recently issued a Notice of Proposed Rulemaking proposing several changes to the COPPA Rule that are intended to respond to changes in technology and online practices.[49]

The FTC also enforces several other rules and statutes that could apply to the activities on an SMVSS. For example, the FTC enforces the Restore Online Shoppers' Confidence Act ("ROSCA"),[50] which prohibits the sale of goods or services on the Internet through negative option marketing without meeting certain requirements for disclosure, consent, and cancellation to protect consumers.[51]

Finally, in addition to the statutes and rules the FTC enforces, state and local laws and regulations govern the privacy practices of SMVSSs, including the Companies and SMVSSs in this report.[52]

---

[47] 16 C.F.R. § 312.7.

[48] *See, e.g., Google LLC*; *United States v. Musical.ly, Inc.*, No. 2:19-cv-01439 (C.D. Cal. Feb. 27, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3004-musically-inc.

[49] *See* COPPA Rule Notice of Proposed Rulemaking, 89 Fed. Reg. 2034 (Jan 11, 2024). The FTC proposed changes that would place new restrictions on the use and disclosure of children's personal information and further limit the ability of companies to condition access to services on monetizing children's data. The proposal aims to shift the burden from parents to providers to ensure that digital services are safe and secure for children. The proposals on which the FTC sought public comment include: (1) requiring separate opt-in for third-party disclosures, such as for targeted advertising; (2) increasing transparency for operators utilizing the support for the internal operations exception; (3) limits on nudging children to stay online; (4) increasing accountability for safe harbor programs; (5) strengthening data security requirements; and (6) limits on data retention. In addition, the FTC has proposed changes to some definitions in the COPPA Rule, including expanding the definition of "personal information" to include biometric identifiers, and stating that the Commission will consider marketing materials, representations to consumers or third parties, reviews by users or third parties, and the age of users on similar websites or services when determining whether a website or online service is directed to children.

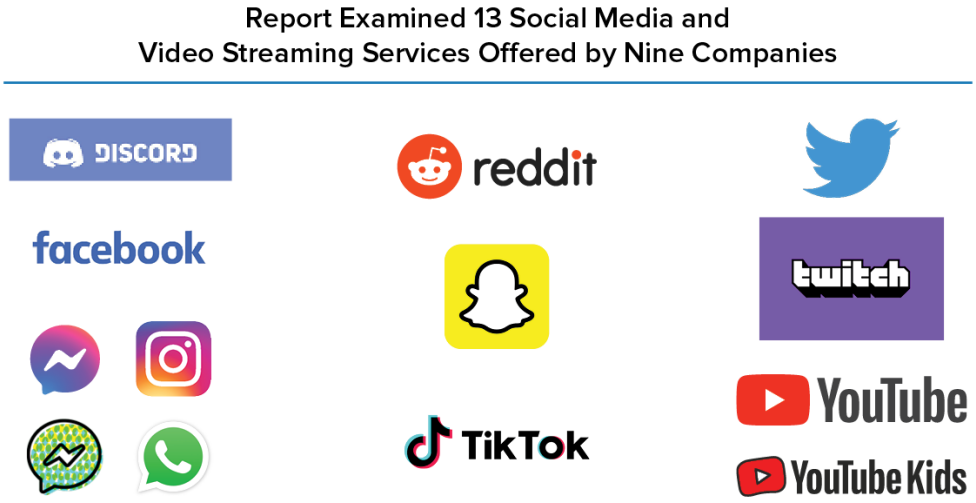
[50] 15 U.S.C. §§ 8401–8405.

[51] A negative option is an offer in which the seller treats a consumer's silence—i.e., their failure to reject an offer or cancel an agreement—as consent to be charged for goods and services. 16 C.F.R. § 310.2(w).

[52] As with Section 5 of the FTC Act, several states have their own consumer protection laws that similarly prohibit unfair or deceptive acts or practices. A number of states have also enacted specific privacy laws, including California, Colorado, Connecticut, Delaware, Illinois (as to biometric information), Indiana, Iowa, Maryland, Montana, Oregon, Tennessee, Texas, Utah, and Virginia, that provide for specified data privacy protections, such as the right for consumers to access data collected or shared about them; the right to correct incorrect or outdated personal information; the right to request deletion of personal information; the right to opt out of the sale of personal information; or the right to opt out of certain automated decision making. *US State Privacy Legislation Tracker: Comprehensive Consumer Privacy Bills*, INT'L ASS'N OF PRIVACY PROF'LS (Dec. 2023), https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.

III. Background Information About the Companies

In December 2020, the Commission issued 6(b) Orders to nine Companies offering SMVSSs.[53] These nine Companies offer some of the best known and popular SMVSSs available to American consumers.[54]



The SMVSSs in our study demonstrate the many ways in which consumers of all ages may interact with or create content online, communicate with other users, obtain news and information, and foster social relationships. For example:

---

[53] Press Release, Fed. Trade Comm'n, FTC Issues Orders to Nine Social Media and Video Streaming Services Seeking Data About How They Collect, Use, and Present Information (Dec. 14, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/12/ftc-issues-orders-nine-social-media-video-streaming-services-seeking-data-about-how-they-collect-use.

[54] Under the Paperwork Reduction Act ("PRA"), 44 U.S.C. §§ 3501-3521, agencies are required to obtain Office of Management and Budget approval after issuing two sequential Federal Register notices before they can solicit responses to identical questions posed to ten or more persons. The FTC tried to ensure a more timely study and report, and as a result opted to seek information from a total of nine recipients. These nine recipients operate several of the largest SMVSSs used by American consumers, but there are nevertheless many other SMVSSs that were not included in our study. Moreover, to ensure compliance with the PRA, the Order instructed the Companies that they ". . . should not seek any responsive information and data from separately incorporated subsidiaries or affiliates or from individuals (other than in their capacity as Your employee or as Your agent). However, You should provide information from separately incorporated subsidiaries or affiliates or from individuals if You already have possession, custody, or control of such information." Appendix A, at 1. Several Companies are part of large corporate families, some with multiple SMVSSs operated by different subsidiaries. As a result, at times staff was not able to obtain complete information regarding SMVSSs if such information was not in the Company's possession, custody, or control, but rather in the possession, custody, or control of a subsidiary or other corporate entity not named as an Order recipient. While this report's findings and conclusions are limited to these nine Companies, it is worthwhile for other actors to consider its recommendations.

- Amazon.com, Inc. is the parent company[55] of the **Twitch** SMVSS, wherein users can watch streamers play video games in real time.[56] In 2022, Twitch reported an average of 31 million daily visitors to its service, most of whom were between 18 and 34 years old.[57]

- ByteDance Ltd. is the ultimate parent company of TikTok LLC, the entity that operates the **TikTok** SMVSS.[58] TikTok enables users to watch and create short-form videos.[59] TikTok reported having 150 million monthly active users in the United States in 2023, up from 100 million monthly active users in 2020.[60]

- Discord Inc. operates the **Discord** SMVSS that provides voice, video, and text communication capabilities to users, by means of community chat rooms known as "servers."[61] In 2023, Discord reported having 150 million monthly active users, with 19 million active community chat rooms per week.[62]

- Meta Platforms, Inc., formerly known as Facebook, Inc.,[63] operates multiple SMVSSs.[64] In 2023, Meta reported having 3 billion users across its services.[65]

---

[55] Press Release, Amazon.com, Inc., Amazon.com to Acquire Twitch (Aug. 25, 2014), https://press.aboutamazon.com/2014/8/amazon-com-to-acquire-twitch.

[56] Twitch states that "Twitch is where millions of people come together every day to chat, interact, and make their own entertainment together." *About*, TWITCH, https://www.twitch.tv/p/en/about/.

[57] *See Audience*, TWITCH, https://twitchadvertising.tv/audience/.

[58] *See* BYTEDANCE, https://www.bytedance.com/en/.

[59] *See Our Mission*, TIKTOK, https://www.tiktok.com/about (stating that "TikTok is the leading destination for short-form mobile video").

[60] David Shepardson, *TikTok hits 150 mln U.S. monthly users, up from 100 million in 2020*, REUTERS (Mar. 20, 2023), https://www.reuters.com/technology/tiktok-tell-congress-it-has-150-million-monthly-active-us-users-2023-03-20/.

[61] *See* DISCORD, https://discord.com/company.

[62] *Id*.

[63] Press Release, Meta Platforms, Inc., Introducing Meta: A Social Technology Company (Oct. 28, 2021), https://about.fb.com/news/2021/10/facebook-company-is-now-meta/.

[64] WhatsApp Inc. is part of the Meta Platforms, Inc. corporate family. WhatsApp Inc. received a separate Order, and is therefore treated as a separate Company for purposes of this report.

[65] *See Our Mission*, META, https://about.meta.com/company-info/. *See also* Press Release, Meta, Meta Reports First Quarter 2023 Results (Apr. 26, 2023), https://s21.q4cdn.com/399680738/files/doc_financials/2023/q1/Meta-03-31-2023-Exhibit-99-1-FINAL-v2.pdf.

- The **Facebook** SMVSS provides users with a communal space to connect to a network of other users by sharing, among other things, text posts, photos, and videos.[66] In March 2023, Meta reported an average of more than 2 billion daily active users and almost 3 billion monthly active users.[67]

- The **Messenger** SMVSS is a messaging application that allows users to communicate via text, audio calls, and video calls.[68] Users of Messenger must have a Facebook account to use Messenger's services.[69]

- The **Messenger Kids** SMVSS is a children's messaging application that allows users to communicate via text, audio calls, and video calls.[70] Parents of Messenger Kids users create accounts for their children through a parent's Facebook account.[71]

- The **Instagram** SMVSS, acquired by Meta Platforms, Inc. in 2012,[72] allows users to share photos and videos with their networks.[73] News reports estimated that as of 2021 there were 1.3 billion users on Instagram.[74]

---

[66] META PLATFORMS, INC., ANNUAL REPORT FORM 10-K (Feb. 2, 2023), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/e574646c-c642-42d9-9229-3892b13aabfb.pdf.

[67] Press Release, Meta Platforms, Inc., Meta Reports First Quarter 2023 Results (Apr. 26, 2023), https://s21.q4cdn.com/399680738/files/doc_financials/2023/q1/Meta-03-31-2023-Exhibit-99-1-FINAL-v2.pdf.

[68] *Supra* note 66.

[69] After enrolling in Messenger, users can choose to deactivate their Facebook accounts. *See Options to use Messenger without a Facebook account*, FACEBOOK, https://www.facebook.com/help/messenger-app/117818065545664.

[70] *Supra* note 66.

[71] *Messenger Kids*, FACEBOOK, https://www.facebook.com/help/messenger-app/213724335832452.

[72] Press Release, Meta Platforms, Inc., Facebook to Acquire Instagram (Apr. 9, 2012), https://about.fb.com/news/2012/04/facebook-to-acquire-instagram/#:~:text=MENLO%20PARK%2C%20CALIF.,cash%20and%20shares%20of%20Facebook.

[73] *About Instagram*, INSTAGRAM, https://help.instagram.com/424737657584573.

[74] Sheera Frenkel et al., *Instagram Struggles With Fears of Losing Its 'Pipeline': Young Users*, N.Y. TIMES (Oct. 16, 2021), https://www.nytimes.com/2021/10/16/technology/instagram-teens.html.

  - The **WhatsApp** SMVSS, acquired in 2014 by Meta Platforms, Inc.,[75] is a messaging platform.[76] WhatsApp reportedly had more than 2 billion users in 2023.[77]

- Reddit, Inc. operates the **Reddit** SMVSS, which provides communities wherein users can discuss their specific interests.[78] News outlets reported that, as of April 2023, approximately 57 million people visit the Reddit platform every day.[79]

- Snap Inc. operates the **Snapchat** SMVSS, which it describes in part as a "visual messaging application that enhances your relationships with friends, family, and the world."[80] Snapchat also includes "Stories," which provides users the ability to "express themselves in narrative form through photos and videos, shown in chronological order, to their friends."[81] Snap Inc. reported having 375 million average daily active users in Q4 2022.[82]

- Twitter, Inc. was a publicly traded company until October 2022,[83] at which time it became a privately held corporation called X Corp. Since that time, X Corp. has operated **X**, formerly known as the **Twitter** SMVSS, which provides users with the ability to share short posts.[84] Twitter, Inc. reported having 217 million average daily users in Q4 2021.[85]

---

[75] Press Release, Meta Platforms, Inc., Facebook to Acquire WhatsApp (Feb. 19, 2014), https://s21.q4cdn.com/399680738/files/doc_news/2014/FB_News_2014_2_19_Financial_Releases.pdf.

[76] *Supra* note 66.

[77] Tatum Hunter, *WhatsApp just added this long-requested feature*, WASH. POST (Apr. 25, 2023), https://www.washingtonpost.com/technology/2023/04/25/whatsapp-multiple-phones/.

[78] REDDIT, https://www.reddit.com/?feed=home.

[79] Mike Isaac, *Reddit Wants to Get Paid for Helping to Teach Big A.I. Systems*, N.Y. TIMES (Apr. 18, 2023), https://www.nytimes.com/2023/04/18/technology/reddit-ai-openai-google.html.

[80] SNAP INC., ANNUAL REPORT FORM 10-K (Feb. 1, 2023), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001564408/c22ae9bd-7418-456e-82d4-48129de1df54.pdf.

[81] *Id*.

[82] *Id*.

[83] Kate Conger, *How Twitter Will Change as a Private Company*, N.Y. TIMES (Oct. 28, 2022), https://www.nytimes.com/2022/10/28/technology/twitter-changes.html.

[84] Twitter was rebranded as "X" in July 2023. *See* Ryan Max & Tiffany Hsu, *From Twitter to X: Elon Musk Begins Erasing an Iconic Internet Brand*, N.Y. TIMES (July 24, 2023), https://www.nytimes.com/2023/07/24/technology/twitter-x-elon-musk.html.

[85] TWITTER, INC., ANNUAL REPORT FORM 10-K (Feb. 16, 2022), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001418091/000141809122000029/twtr-20211231.htm.

- YouTube, LLC is wholly owned by Google LLC, with Alphabet Inc. as the ultimate parent. Google LLC operates YouTube's two SMVSSs.

    - The **YouTube** SMVSS is a video sharing product. As of February 2021, YouTube, LLC reported that "over two billion logged in users [come] to YouTube every month . . . ."[86]

    - The **YouTube Kids** SMVSS, first introduced in 2015,[87] is a children's video product with family-friendly videos and parental controls.[88] As of February 2021, YouTube, LLC reported that YouTube Kids had more than 35 million weekly viewers.[89]

While the SMVSSs in this report are generally "zero price" (or have free versions available) for the end user – meaning they require no money from consumers to sign up, or to create an account, for the basic version of the product – firms monetize (or profit off of) these accounts through data and information collection. This report examines the practices that enable these Companies to generate

[86] Neal Mohan, *Investing to empower the YouTube experience for the next generation of video*, YOUTUBE OFFICIAL BLOG (Feb. 17, 2021), https://blog.youtube/inside-youtube/neal-innovation-series/.

[87] Shimrit Ben-Yair, *Introducing the newest member of our family, the YouTube Kids app – available on Google Play and the App Store*, YOUTUBE OFFICIAL BLOG (Feb. 23, 2015), https://blog.youtube/news-and-events/youtube-kids/.

[88] YOUTUBE KIDS, https://www.youtube.com/kids/.

[89] *Supra* note 86.

billions of dollars in revenue while primarily offering free services.[90] The answer lies in the ways in which the Companies monetize and use user and non-user data, especially through advertising.[91]

In particular, our report finds that most of the Companies' revenue from the SMVSSs was derived by serving or displaying advertisements ("Digital Advertising Service"),[92] and that all these Digital Advertising Services provided ad-targeting capabilities.[93] These Digital Advertising Services were typically business-to-business services that consumers did not interact with directly but that catered to third-party advertisers and allowed them to advertise both on and off of the relevant SMVSS. The Companies charged third-party advertisers to use their Digital Advertising Service(s), including by allowing the advertisers access to valuable information that SMVSSs compiled about users, including

---

[90] For Q1 2023, Amazon.com, Inc. reported net sales of $3.2 billion. Press Release, Amazon.com, Inc., Amazon.com Announces First Quarter Results (Apr. 27, 2023), https://s2.q4cdn.com/299287126/files/doc_financials/2023/q1/Q1-2023-Amazon-Earnings-Release.pdf.

News outlets reported that ByteDance's 2022 earnings surpassed $80 billion. Zheping Huang, *ByteDance Matches Tencent's $80 Billion Sales After TikTok Boom*, BLOOMBERG (Apr. 3, 2023), https://www.bloomberg.com/news/articles/2023-04-03/bytedance-matches-tencent-s-80-billion-sales-after-tiktok-boom#xj4y7vzkg.

For Q1 2023, Meta Platforms, Inc. reported $28.65 billion in revenues. Press Release, Meta Platforms, Inc., Meta Reports First Quarter 2023 Results (Apr. 26, 2023), https://s21.q4cdn.com/399680738/files/doc_financials/2023/q1/Meta-03-31-2023-Exhibit-99-1-FINAL-v2.pdf.

Snap Inc. reported revenues of $4.6 billion in 2022. Press Release, Snap Inc., Snap Inc. Announces Fourth Quarter and Full Year 2022 Financial Results (Jan. 31, 2023), https://investor.snap.com/news/news-details/2023/Snap-Inc.-Announces-Fourth-Quarter-and-Full-Year-2022-Financial-Results/default.aspx.

Twitter, Inc. reported revenues of $5.08 billion in 2021. *Supra* note 85.

For Q1 2023, Alphabet Inc. reported $69.8 billion in revenues. Press Release, Alphabet Inc., Alphabet Announces First Quarter 2023 Results (Apr. 25, 2023), https://abc.xyz/assets/c1/25/dca115b845bd834819846bf67068/2023q1-alphabet-earnings-release.pdf. Alphabet Inc. reported making more than $29 billion in revenues from YouTube ads in 2022. ALPHABET INC., ANNUAL REPORT FORM 10-K (Feb. 2, 2023), https://abc.xyz/assets/9a/bd/838c917c4b4ab21f94e84c3c2c65/goog-10-k-q4-2022.pdf.

[91] Most of the Companies with advertising services reported that the majority of their revenues came from advertising.

[92] The Order defines "Digital Advertising Service" to include "each Company product or offering that serves or displays, or Company service Relating to the service or display of, advertisements through an application or website on any device (e.g., personal computer, iOS device, Android device, etc.)." Appendix A, Definition O.

[93] Targeted advertising, also known as behavioral or personalized advertising, is where advertisers can target specific users or groups based on specific criteria. The goal of targeted advertising is to direct advertisements to users or groups that will find the advertisement more relevant. Contextual advertising involves non-personalized advertising shown as part of a consumer's current interaction with a website or mobile application. Contextual advertising does not include the disclosure of a consumer's personal information to other third parties, nor does it include the use of a consumer's personal information to build a profile about the consumer or to otherwise alter the consumer's experience outside the current interaction with a website or mobile application. *See, e.g.*, *GoodRx Holdings, Inc.*, Provision I.B of Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief.

their "Personal Information"[94] and "Demographic Information,"[95] activities, and interests. The Companies also generally offered advertisers multiple ways to target users with advertisements for products and services that users saw or interacted with while using the SMVSS. This included allowing advertisers to identify and target particular audiences of users, such as users who fell into specific demographic categories. The specific objective of targeted advertising varied, although ultimately the goal was that the user would respond to the advertisement in some fashion. Providing Digital Advertising Services can provide an incentive to compile extensive information about users, both on- and off-line, to offer targeted advertising and increase advertising revenues for the Company. As a result, while all of these SMVSSs are "free" in the sense of being zero price (or have free versions available), consumers effectively pay through their data and information.[96]

A small number of the Companies did not have Digital Advertising Services, did not have any advertising revenue, and did not monetize user data for advertising. As a result, such Companies relied on other means to make money, such as the sale of subscription services, add-on features, or services offered to business customers that did not relate to advertising. While these non-advertising services and features, including the sale of subscription services, did raise revenue for the Companies without a Digital Advertising Service, in the aggregate these figures were significantly less than the revenues for Companies with a Digital Advertising Service.

---

[94] The Order defines "Personal Information" as "information about a specific individual or Device, Including: (1) first and last name; (2) home or other physical address, Including street name and name of city or town, or other information about the location of the individual, Including but not limited to location from cellular tower information, fine or coarse location, or GPS coordinates; (3) Email address or other online contact information, such as an instant Messaging user identifier or screen name; (4) telephone number; (5) a persistent identifier, such as a customer number held in a 'cookie,' a static Internet Protocol ('IP') address, a device identifier, a device fingerprint, a hashed identifier, or a processor serial number; (6) nonpublic Communications and content, Including, but not limited to, e-mail, text messages, contacts, photos, videos, audio, or other digital images or audio content; (7) Internet browsing history, search history, or list of URLs visited; (8) video, audio, cable, or TV viewing history; (9) biometric data; (10) health or medical information; (11) Demographic Information or (12) any other information associated with that User or Device." Appendix A, Definition Z.

[95] The Order defines "Demographic Information" as "characteristics of human populations, such as age, ethnicity, race, sex, disability, and socio-economic information." Appendix A, Definition M.

[96] Snap Inc. stated in its 2023 10-K "individuals are becoming increasingly resistant to the processing of personal data to deliver behavioral, interest-based, or targeted advertisements . . . ." SNAP INC., ANNUAL REPORT FORM 10-K (Feb. 1, 2023), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001564408/c22ae9bd-7418-456e-82d4-48129de1df54.pdf

IV. Data Practices

The privacy of consumers' data collected online has long been a concern to the Commission, for a variety of reasons.[97] Surveys have found that consumers are concerned and feel they lack control over online data collection practices,[98] or may not fully comprehend the breadth of online data collection practices.[99] Consumers' concern and perceived lack of control extends to the data collection practices of SMVSSs.[100] Moreover, the potential harms that can come from unfettered data collection practices are significant.[101]

---

[97] *See, e.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; Fed. Trade Comm'n, Commercial Surveillance and Data Security Rulemaking (Aug. 11, 2022), https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking.

As discussed in the Executive Summary, the term "privacy" in this report is intended to encompass unknown, unexpected, or unwanted surveillance, collection, and use of, or inference from, consumers' information, over which companies have given consumers little control, access, or choice.

[98] *See* Colleen McClain et al., How Americans View Data Privacy, PEW RES. CTR. (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/ (finding that 73% of U.S. adults surveyed believe they have little to no control over what companies do with their data).

[99] *See generally id.* (finding that 67% of U.S. adults surveyed said they do not understand what companies are doing with their data).

[100] *See generally* Brandon Jarman, *Verizon Specials Social Privacy Survey Report 2022*, VERIZON BLOG (Sept. 18, 2023), https://www.verizonspecials.com/resources/social-media-personal-data-privacy-survey/ (finding that 81% of those surveyed were at least somewhat concerned about their privacy on social media).

[101] *See, e.g.*, Caitriona Fitzgerald et al., *The State of Privacy: How state "privacy" laws fail to protect privacy and what they can do better*, ELECTRONIC PRIVACY INFO. CTR. (Feb. 2024), https://epic.org/wp-content/uploads/2024/01/EPIC-USPIRG-State-of-Privacy.pdf ("The more data companies collect about us, the more our data is at risk. When companies hold your data, the greater the odds it will be exposed in a breach or a hack and end up in the hands of identity thieves, scammers, or shadowy companies known as data brokers that buy and sell a huge amount of data about Americans."); Jennifer King & Caroline Meinhardt, *Rethinking Privacy in the AI Era*, STANFORD UNIV. (Feb. 2024), https://hai.stanford.edu/sites/default/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf ("Largely unrestrained data collection poses unique risks to privacy that extend beyond the individual level—they aggregate to pose societal-level harms that cannot be addressed through the exercise of individual data rights alone."); Memorandum Decision and Order on Motion to Dismiss First Amended Complaint, *Fed. Trade Comm'n v. Kochava, Inc.*, No. 2:22-cv-00377-DCN (D. Idaho Feb. 3, 2024) (holding that the FTC alleged facts sufficient to show that Defendant Kochava's "data sales harm consumers in two distinct ways. First, by putting them at an increased risk of suffering secondary harms, such as stigma, discrimination, physical violence, and emotional distress. And second, by invading their privacy."); Justin Sherman et al., *Data Brokers and the Sale of Data on U.S. Military Personnel*, DUKE UNIV. (Nov. 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf (finding that it was not difficult to obtain sensitive data about active-duty members of the military and their families, and veterans, and that "[a]ccess to this data could be used by foreign and malicious actors to target active-duty military personnel, veterans, and their families and acquaintances for profiling, blackmail, targeting with information campaigns, and more."); *Social Media Safety Index 2023*, GLAAD (2023), https://glaad.org/publications/social-media-safety-index-2023/ ("To protect

With these concerns in mind, the Commission's Order sought information from the Companies regarding their data collection, use, disclosure, minimization, retention, and deletion practices.[102] The Order also sought information regarding the Companies' practices with respect to more sensitive information, such as Demographic Information.[103]

In this section we will review the Companies' reported practices with respect to user data. First, we will review the Companies' reported data collection, use, and disclosure practices, including: the types of data collected; where and how the Companies collected data; what the Companies used the data for; and which entities the Companies shared such data with. Second, we will examine the Companies' reported data minimization, retention and deletion policies and practices. Third, we examine consumer rights provided for under the European Union's General Data Protection Regulation, and if the Companies also afforded such consumer rights to U.S. users.[104] We conclude with key findings.

A. Data Collection, Use, and Disclosure

The Companies all reported collecting data, including Personal Information,[105] from and about consumers. Several aspects of these data practices are less visible to users of SMVSSs. These include:

- the nature and volume of the Companies' data collection;
- their methods of data collection;
- their sources of data collection;
- how and with whom they shared data;

LGBTQ users from surveillance and discrimination, platforms should reduce the amount of data they collect and retain."); *Amazon.com, Inc.* (alleging that "users suffer injuries to their privacy due to the unauthorized use of their information."); Samantha Lai & Brooke Tanner, *Examining the intersection of data privacy and civil rights*, BROOKINGS INST. (July 18, 2022), https://www.brookings.edu/articles/examining-the-intersection-of-data-privacy-and-civil-rights/ (stating that federal privacy legislation is needed to address "commercial surveillance practices that enable discriminatory advertising, racially biased policing, and the outing or surveillance of historically marginalized groups."); Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022) ("Many privacy violations involve broken promises or thwarted expectations about how people's data will be collected, used, and disclosed. The downstream consequences of these practices are often hard to determine . . . People might be flooded with unwanted advertising or email spam. Their expectations may be betrayed, resulting in their data being shared with third parties that may use it in detrimental ways—but precisely when and how is unknown."); Support King, LLC, No. C-4756 (Dec. 21, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3003-support-king-llc-spyfonecom-matter (alleging that "[s]talkers and abusers use mobile device monitoring software to obtain victims' sensitive personal information without authorization and monitor surreptitiously victims' physical movements and online activities. Stalkers and abusers then use the information obtained via monitoring to perpetuate stalking and abusive behaviors, which cause mental and emotional abuse, financial and social harm, and physical harm, including death.").

[102] *See* Appendix A, Specification Nos. 10—20.

[103] *See* Appendix A, Specification Nos. 39—41.

[104] The Order requested that the Companies "Describe in Detail all material changes made by the Company to comply with the European Union's General Data Protection Regulation, Including whether those changes apply exclusively to users in the European Union or also to users in the United States . . . ." Appendix A, Specification 52.

[105] *See supra* note 94.

- how they used and allowed others to use the data; and
- whether they placed any restrictions on the use and disclosure of the data.

Responses to the Order also revealed how these data practices differed among the Companies. The responses revealed that the Companies generally: collected enormous amounts of data about users and non-users alike, regarding both activity on and off of the SMVSSs; collected such data from a variety of sources, both on and off of the SMVSSs; used data for a multitude of purposes; and engaged in data sharing with various affiliated and non-affiliated entities.

1. The Companies Generally Collected Vast Amounts of Data About Users and Non-Users

The Companies examined for this report collected data not only about consumers' activity on the SMVSSs[106] but also about consumers' activity *off* of the SMVSSs. Our report finds that the Companies collected a variety of data about consumers vis-à-vis their activity on, and interaction with, various SVMSSs, including:

- **Demographic Information**: Most Companies collected or inferred Demographic Information regarding their SMVSS users. Only a few Companies reported not collecting or inferring any Demographic Information about their SMVSS users.[107] For those that did collect or infer Demographic Information, they most frequently collected or inferred users' age, gender, and language. Some Companies reported collecting or inferring other forms of Demographic Information, including information regarding their SMVSS user's household, such as education, income, marital status, and parental status.[108] Most Companies reported not collecting or inferring Demographic Information about non-users or non-users' households.

- **User Metrics**: "User Metrics" are data regarding a user's interaction with an SMVSS network, such as the number of other SMVSS users one follows or is otherwise associated with.[109] The Companies reported collecting between five and 135 User Metrics on their SMVSSs, with an average of 28 per SMVSS. While User Metrics may seem innocuous (e.g., an SMVSS's total number of daily active users), such data can still convey detailed information about a particular user. For example, most Companies collected the number of messages sent or received by a user. While this is not the same as tracking the content of those messages, it nevertheless

---

[106] All SMVSSs offered consumers the ability to create an account to access the SMVSS's services. Some SMVSSs made their services available without requiring an account.

[107] Some of the SMVSSs that reported not collecting or inferring any Demographic Information about their users nevertheless obtained third-party audience segments that could include segments based on age, household income, etc.

[108] Very few SMVSSs reported collecting or inferring information regarding a user's race or ethnicity.

[109] The Order defines "User Metric" as "each metric for user interaction with any web site or application owned or operated by any Person (Including the Company) on any device (e.g., personal computer, iOS device, or Android device)." Appendix A, Definition NN.

demonstrates that most Companies were monitoring users' non-public messages sent or received using their SMVSSs.

- **Privacy Preferences**: Most Companies did not collect data on users' changes or updates to privacy settings on their SMVSSs.[110] Only one Company's SMVSS kept track of users' interactions with privacy and ad personalization settings. No Company tracked all of a user's changes or updates to privacy settings, or requests related to porting, access, accuracy, and deletion.[111] Overall, the Companies' tracking of users' privacy preferences was inconsistent. The most tracked privacy preferences were access and deletion requests. The least tracked were correction requests. Some Companies stated that they only started tracking this information in early 2020 in response to the California Consumer Privacy Act of 2018 ("CCPA").[112] Significantly, the failure of most entities to track users' changes and updates to privacy settings, in contrast to their typical practice of tracking user behavior, demonstrates a relative lack of attention to consumers' privacy preferences.

Our report also finds that the Companies received different types of information regarding consumers' activity off of their SMVSSs, such as consumers' activity on *other* SMVSSs. The Order called for information regarding whether the Companies track users' usage of other SMVSSs.[113] Several Companies allowed users to connect their account to accounts on another SMVSS or otherwise integrate or share content. When this happened, the Company received information about the user's profile on the other SMVSS. Several Companies stated that they did not intentionally track a user's activity on other SMVSSs. Companies nevertheless received data on a user's activity on other SMVSSs where the other SMVSS became a business customer of the Company (e.g., for advertising purposes) or if they received a referring URL (e.g., consumer user arrived at content from a link posted on another SMVSS). Moreover, the Companies' responses did not account for tracking that occurred on other SMVSSs that were part of the same corporate family (e.g., when entities within the same corporate family operate different SMVSSs and track user activities across those SMVSSs).

Some consumer information collected by the Companies was a combination of data regarding a user's activity on *and* off of the Company's SMVSS. That is, when consumers used an app or website unrelated to the SMVSS, the unrelated apps or websites tracked information about the user's activity and shared it with the SMVSSs. For example:

---

[110] Specification 19 of the Order requires, among other things, that the Companies provide "the number of users who (a) made changes to their privacy settings; (b) requested access to their data; (c) requested correction of their data; (d) requested to port their data; or (e) requested to delete their data." Appendix A, Specification No. 19.

[111] *See infra* Section IV.C for information regarding privacy rights afforded to consumers.

[112] Cal. Civ. Code § 1798.100 et seq.

[113] Specification 6 of the Order requests, in part, "[f]or each [SMVSS] identified . . . [the] [monthly active users] . . . also active on another [SMVSS] provided or sold by any Person other than the Company . . . and Identifying such other [SMVSS])." Appendix A, Specification No. 6.

- **Personal Information**: While the Order did not explicitly request that the Companies report all the types of Personal Information collected, answers to other Order specifications demonstrate that the SMVSSs collected Personal Information about users and non-users, including email address, URLs visited, Demographic Information, and other information associated with a user or device.

- **User Attributes:** "User Attributes" refer to user characteristics or categorizations.[114] The most common User Attributes collected by the Companies were: country; region (including state/city);[115] language; and user interests.[116] With respect to the quantity of User Attributes collected by the Companies, the Companies collected from zero User Attributes to an indeterminate number of User Attributes.[117] For some Companies, it was clear that all User Attributes were collected from a user's interaction with the SMVSS, including such data elements as the primary language of the user. These Companies were able to succinctly list all the User Attributes they collected or used. For other Companies, many of their User Attributes came from third-party data sets, such as interest categories primarily utilized for targeted advertising. These Companies were either only able to provide high-level categories of the User Attributes collected or produced spreadsheets with thousands of User Attributes. And other Companies could not, or would not, disclose where the information originated from. For example, one Company stated that it collected User Attributes, but could not provide the values associated with each User Attribute.

  Companies that did not obtain User Attributes via third parties were generally more capable of relaying to the FTC the User Attributes collected, whereas those that received User Attributes from third parties exhibited an inability to fully account for all of the User Attributes in their possession. That such Companies cannot succinctly identify all of the User Attributes they track

---

[114] The Order defines "User Attribute" as "each attribute or categorization of any user (e.g., age, gender, country, language, categorizations based on user interests, or categorizations based on other user behavior) of any Social Media and Video Streaming Service that is tracked or used by the Company for any purpose, Including, but not limited to, the provision or sale of any Social Media and Video Streaming Service or advertising." Appendix A, Definition LL.

[115] The Order did not include specifications requesting specific information regarding the Companies' practices with respect to location data or geolocation tracking. However, as evidenced here, it is a type of user data that many companies collect and use. The Commission's commitment to addressing the privacy and security concerns related to location data and tracking is reflected in its recent work regarding these areas. *See, e.g.*, InMarket Media, LLC, No. C-4803 (F.T.C. May 1, 2024); *X-Mode Social, Inc.*; *Fed. Trade Comm'n v. Kochava, Inc.*, No. 2:22-cv-00377-DCN (D. Idaho Aug. 29, 2022); Kristin Cohen, *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, FED. TRADE COMM'N (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

[116] *See* User Interests discussion below for more detail.

[117] In fact, one Company informed staff that it could only provide data categories, stating that such categories "reflect[] the greatest level of specificity for User Attributes tracked by the Company." It appears that the Companies that received third-party data sets were most likely to report that providing a succinct list of User Attributes collected was not feasible.

calls into question whether they can adequately prevent privacy abuses, unlawful discrimination, and other serious harms described throughout this report.

- **Shopping Behavior**: Most Companies stated that they deliberately collected information regarding consumers' shopping behaviors. A minority of Companies, including all Child-directed[118] SMVSSs,[119] stated that they did not deliberately collect this information, but admitted they could have become aware of a user's shopping behaviors and interests via the user's interaction with the SMVSS. For those that did collect this information, the types of information collected varied across the Companies, including information about consumers' actual purchases and shopping behavior as well as inferred shopping interest segments. One Company stated that it did not collect information regarding users' shopping behaviors, albeit allowing consumers to make purchases directly through the SMVSS.

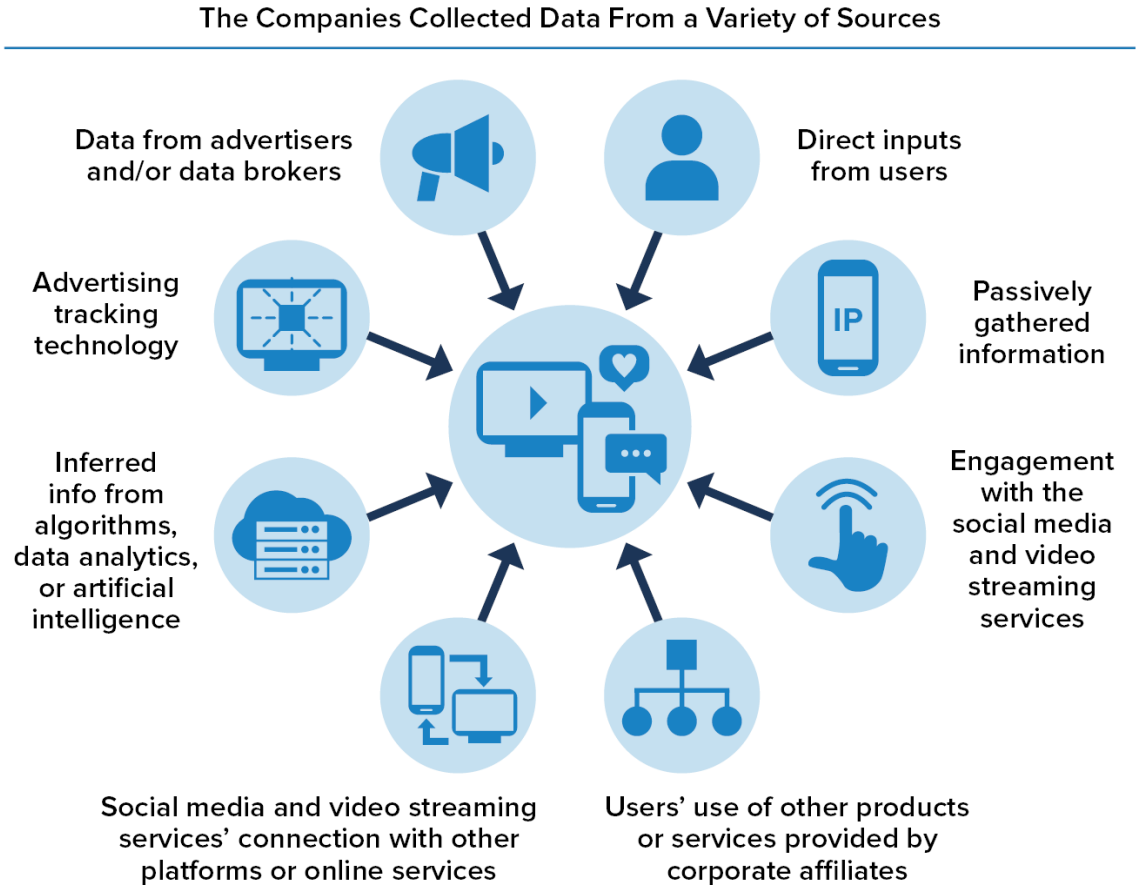
- **User Interests**: Several Companies reported having information regarding users' interests. The Companies primarily used such user interests for targeted advertising purposes. Some Companies provided several interest categories, and several acknowledged that each category could have many more specific subparts. For example, a Company may have had a user interest category of "food and drink/beverages," but within that category were a large set of subgroups, such as "beer and spirits," "fast food," or "bars and nightlife." Of particular interest, some Companies revealed user interest categories that are more akin to Demographic Information. For example, some Companies' user interest categories revealed parental status (e.g., user interest category for "baby, kids and maternity") or marital status (e.g., "newlyweds" or "divorce support"). While such user interests may, at first glance, seem innocuous, the particularity of user interest categories often would have allowed the Company to infer more (and sometimes much more) information about a consumer.

[118] The Order defines "Child" or "Children" as "individuals under the age of thirteen (13)." Appendix A, Definition I.

[119] Some Companies indicated in their responses that they have SMVSSs that are directed to Children.

2. The Companies Generally Collected Data from a Variety of Sources, Both On and Off of the SMVSSs

The data collection practices employed by the Companies went much further both on and off of the SMVSS, and sometimes implicated consumers who are not even registered users of an SMVSS. Our study found that the Companies collected data from consumers in a myriad of ways, including:



- **Direct inputs from SMVSS users themselves**. For the Companies, this typically came from information that a user actively submitted to an SMVSS (e.g., profile information[120]). One Company reported receiving information from consumers who completed voluntary surveys or interviews. For the most part, consumers may have expected this form of data collection as it involved consumers' direct involvement and participation. But at least one Company engaged in in-app keystroke tracking (claiming it helped detect security incidents and fraud), which consumers would likely not have expected.

[120] The information that an SMVSS user submits to an SMVSS differs across the Companies, and even across SMVSSs operated by the same Company. For example, a Facebook profile has specific fields wherein a user can submit information regarding their "Work," "Education," "Places Lived," "Contact info," "Basic info," and "Relationship(s)." In contrast, a TikTok profile has an open-ended "bio" space where users can choose what information they submit.

- **Passively gathered information**. Several Companies reported the collection of different types of information regarding a user's access to the SMVSS, such as IP address and device data. A few Companies acknowledged that they used such information for targeted advertising purposes. While many consumers might expect that the Companies would have needed to collect information regarding their device or internet connection to provide the SMVSS, it is unlikely that consumers would expect such information to have also been used for separate, unrelated purposes.

- **SMVSS users' engagement with the SMVSS**. Based on the Companies' responses, information attributed to a user would be based off of a user's interactions with content on the SMVSS, such as likes and searches. For example, some Companies inferred information about a user (such as the user's interests) based on the content the user shared or posted on the SMVSS, or content the user otherwise engaged with (e.g., content a user watched or searched for).[121] To the extent that an SMVSS allowed users to make purchases directly through the platform, Companies also often collected users' shopping behavior.

- **SMVSS users' use of, and engagement with, other products or services provided by corporate affiliates.** At least one Company reported collecting information not only from a user's interactions with the SMVSS, but also from a user's interactions with all other online services within the Company's corporate family.

- **SMVSS connection with other platforms or online services.** In addition, as previously discussed, several Companies allowed users to connect their account to accounts on other SMVSSs, or otherwise integrate or share content, thus establishing another means by which the Companies could collect data.

- **Algorithms, Data Analytics, or AI**:[122] Many Companies reported inferring user information through the use of Algorithms, Data Analytics, or AI. Such Companies most often reported inferring a user's age or age range using such technology. A few Companies reported using systems on some SMVSSs to automatically identify Children and several more reported using such systems to identify "Teens."[123]

---

[121] User Engagement information could also reveal who a user is interacting with or following (i.e., actual people in a user's social network).

[122] *See* Section VI for more information regarding the Companies' use of Algorithms, Data Analytics, or AI.

[123] The Order defines "Teen" or "Teens" as "individuals between the ages of thirteen (13) and seventeen (17), inclusively." Appendix A, Definition JJ.

- **Advertising technology**:[124] Advertising technology, also known as ad tech, are tools that are used in conjunction with online advertising. A few Companies reported making ad tech, such as pixels, software development kits ("SDKs"),[125] and application programming interfaces ("APIs"),[126] available for advertisers to use.[127] These are often pieces of code that the SMVSSs made available to their advertisers. When advertisers integrated such ad tech into the advertiser's[128] website(s) or mobile app(s), detailed information about an individual and their activity on those websites/mobile apps would be relayed back to the Company and was used to deliver targeted advertising to a user on the SMVSS.[129]

- **Data obtained from third parties:** There was a trend among the Companies to receive various information on users, and non-users, from third parties. Third parties that provided information to the Companies included:

    - **Advertisers**: Most Companies with a Digital Advertising Service allowed advertisers to import customer lists for targeted advertising purposes. Once a customer was matched to an SMVSS user the advertiser could either direct advertisements to that user or to members of a "lookalike audience."[130]

---

[124] *See* Section V for more information on the Companies' use of advertising technology.

[125] An SDK, or software development kit, is "a set of platform-specific building tools for developers . . . components like debuggers, compilers, and libraries to create code that runs on a specific platform, operating system, or programming language." *What is an SDK?*, AMAZON AWS, https://aws.amazon.com/what-is/sdk/#:~:text=A%20software%20development%20kit%20(SDK,run%20software%20in%20one%20place.

[126] An API, or application programming interface, is "a set of defined rules that enable different applications to communicate with each other. It acts as an intermediary layer that processes data between systems, letting companies open their application data and functionality to external third-party developers, business partners, and internal departments within their companies." *What is an API?*, IBM, https://www.ibm.com/topics/api.

[127] Most of these Companies offered their own ad tech to be used, but at least one Company reported offering third-party ad tech.

[128] Advertisers are any entity that is interested in advertising on an SMVSS (e.g., a clothing company that offers online shopping as well as brick-and-mortar stores), including well-known and popular companies consumers engage with frequently.

[129] Pixels and APIs are not limited to being used for advertising purposes. In fact, a few Companies reported providing APIs to business customers that could use them to import customer information.

[130] *See* Section V for more information on the Companies' advertising practices.

- **Data Brokers**:[131] Most Companies with a Digital Advertising Service purchased data sets from data brokers and others. Such data sets could focus on varying attributes, such as household income, location, and interests. All the Companies that purchased these data sets reported using such information for targeted advertising purposes, wherein advertisers can opt to target certain audiences developed in part from the purchased data sets. For example, such data sets could have informed which SMVSS users fit into a particular interest category that an advertiser would like to target (e.g., a pet food company would like to target SMVSS users who are pet owners).

3. The Companies Generally Used Consumer Data for a Variety of Purposes

The Companies reported using consumer information for several purposes, including:

- **Advertising**: Those Companies engaged in advertising generally used consumers' information for targeted advertisements (including assigning consumers to interest-based categories). Section V goes into more detail regarding the Companies' advertising practices.

- **Algorithms, Data Analytics, or AI**: Generally, Companies that used Algorithms, Data Analytics, or AI would have consumers' information ingested by Algorithms, Data Analytics, or AI (such as machine learning tools) for various purposes (e.g., advertising, content promotion). Section VI goes into more detail regarding the Companies' use of Algorithms, Data Analytics, or AI, including machine learning, and other automated tools.

- **Business Purposes**: Some Companies reported using data, including the data they received from third-party advertisers that used their Digital Advertising Services, for their SMVSS's own business purposes, such as research and development, and ad optimization. Only a few Companies said that they would use anonymized data whenever they could still meet the business purpose without using identifiable data.

- **User Engagement:** Beyond advertising, the Companies generally reported using data to maintain and enhance User Engagement through content promotion. Most Companies reported using information from the SMVSS users to determine what content to present to such users, including: User Engagement[132] (e.g., what content a user has already engaged with on an SMVSS); User Metrics (e.g., number of connections, such as friends or followers, on an SMVSS); User Attributes (e.g., language, location, user interests, device information); and Demographic Information (e.g., age, gender). Some Companies reported that information about a user's friends or other connections on the SMVSS also influenced the content promoted to the

[131] *See generally* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[132] *See supra* note 13.

user. A few Companies reported using other information, such as contacts from a user's address book (if shared) or the content a user shared from other SMVSSs, to determine what content to present to a user.

- **Infer Other Information**: Most of the Companies also reported using user information to infer or deduce even more information about the user. Of those Companies that reported doing so, most reported inferring different types of Demographic Information[133] (most often age or gender) and User Attributes (most often user interests).

- **Analyzing User Engagement**: Most Companies utilized the User Metrics they collected, often the average daily or monthly users, to study and analyze User Engagement. The Companies generally reported that they studied and analyzed User Engagement in order to keep users engaged with their SMVSS's content and on the service, but several also reported studying and analyzing User Engagement in order to evaluate or develop product features or serve advertising to relevant users. Many Companies analyzed User Engagement by looking at User Attributes (e.g., content viewed). One Company reported pseudonymizing User Attributes before using such data to analyze User Engagement.

4. The Companies Generally Shared Data with a Variety of Entities, Including Affiliates and Other Third Parties

SMVSSs design the systems and procedures they use to share consumers' data. The systems and procedures they implement are often opaque, leaving consumers in the dark about the breadth of sharing, the parties with whom the Companies share information, and the purposes of that disclosure.

The Order required that the Companies, with respect to the sharing of Personal Information, "Identify those entities and Describe in Detail the types of Personal Information and purposes for such sharing . . . ."[134] Some Companies reported sharing data broadly with affiliates and third-party entities but provided limited transparency on the specifics in their responses.[135] No Company provided a comprehensive list of all third-party entities that they shared Personal Information with. Some Companies provided illustrative examples, whereas others claimed that this request was impossible. A few Companies provided only the names of third-party entities with which the Company had entered a formal contract, thus omitting third parties that the Companies shared with that were not subject to contracts. Altogether, the Companies' responses lacked clear explanations or specificity regarding the

[133] A few Companies reported inferring Demographic Information well beyond age and gender, such as marital status, parental status, household income, education, and home ownership.

[134] *See* Appendix A, Specification Nos. 14, 15.

[135] The Order requested, among other things, that the Companies identify by name all third-party entities that the Companies shared Personal Information with. Appendix A, Specification No. 15.

exact use cases for sharing with each entity.[136] This lack of transparency could indicate an inability or unwillingness to account for the extent of those practices because consumers' data was shared so broadly.

- **Children or Teens**: Most of the Companies did not report implementing any additional safeguards around sharing information collected from Children or Teens.[137] Most Companies stated that their SMVSSs were not directed to Children and that they did not knowingly have any information collected from Children.[138] Because of this, these Companies contended there is no need for different sharing practices because all information would have been from individuals thirteen or over. Such Companies came to this conclusion despite evidence indicating that Children are on their SMVSSs.[139] Moreover, no Companies reported having sharing practices that treat the information collected from a user known to be aged thirteen to seventeen differently from an adult's information. Among other things, this shows that any privacy protections that were present for Children on a given SMVSS disappeared the moment that Child turned thirteen.[140]

- **Affiliates or Company-Branded Entities**: Most Companies acknowledged that they shared users' Personal Information with affiliates and other company-branded entities. Of the Companies that reported sharing Personal Information, the most commonly reported purposes were to measure User Engagement or growth, to support product or service development, and for safety and security reasons. Less commonly reported purposes for sharing Personal Information included for tax and legal compliance, and to facilitate payment processing.

---

[136] For example, many responses would generally identify a category of third-party entities (e.g., vendor) along with a vague purpose (e.g., legal compliance) for such sharing, rather than providing the detailed description required by the Order. When the FTC asked for clarification, several Companies simply restated their prior answer without providing additional information, or altogether refused to respond to the FTC's follow-up request.

[137] *See* Section VII for more information on the Companies' practices with respect to Children and Teens. Only a few Companies reported engaging in different sharing practices with respect to Personal Information collected from users under thirteen years of age. Generally speaking, such sharing was more limited in nature than the sharing of adult user data.

[138] If an online website or service is directed to Children or has actual knowledge that it is collecting or maintaining personal information from Children, then it must comply with the COPPA Rule. 16 C.F.R. pt. 312. Some Companies reported more limited external sharing practices with respect to information generally collected from Child-directed services.

[139] *See generally* Press Release, Lero, Children can bypass age verification procedures in popular social media apps by lying (Jan. 25, 2021), https://lero.ie/news-and-events/children-can-bypass-age-verification-procedures-popular-social-media-apps-lying.

[140] *See* Section VII for more information on the Companies' practices with respect to Children and Teens.

- **Third Parties**: Most Companies reported sharing users' Personal Information with third parties.[141] The three types of entities the Companies most often reported sharing Personal Information with were: service providers and vendors, developers, and law enforcement.

  Most Companies stated that the purpose of sharing with a service provider/vendor was to facilitate the operation and functioning of the SMVSS (e.g., website hosting and offering certain functionalities). However, some Companies also reported sharing Personal Information with service providers/vendors for the purpose of data analytics, something that arguably would not be necessary for the SMVSS's functioning. The information provided by Companies that reported sharing Personal Information with service providers/vendors for data analytics purposes generally was vague and did not explain what was meant by data analytics.

  Several other Companies reported sharing information with other third-party entities for advertising, marketing, or measurement purposes. One Company that reported that it did not have a Digital Advertising Service nevertheless reported sharing users' Personal Information with partners for the Company's own advertising purposes (e.g., digital advertisements off of the SMVSS promoting the Company).

  Of the Companies that did identify the third parties with whom they shared Personal Information, many of these third parties were located outside of the United States. For example, some third parties that received users' Personal Information were located in China, Hong Kong, Singapore, India, the Philippines and Cyprus. Such sharing raises concerns about the Companies sharing U.S. consumers' Personal Information in a way that may expose that data to potential collection by foreign governments.

- **Researchers and Academics**: Most Companies reported that academics or researchers could access Personal Information or other information held by their SMVSSs. A few Companies stated that they would share information with researchers only when the researchers were conducting research on behalf of the SMVSS. Some Child-directed SMVSSs allowed for such sharing, while others did not. Of the SMVSSs that shared with academics/researchers, all shared publicly available information. A few stated that they would share private information with academics/researchers only if users consented to such sharing. A few Companies reported that they would not share private information with academics/researchers at all. Most of the sharing done by the Companies occurred via APIs, but some Companies' SMVSSs would more

[141] The Order requested that the Companies "Describe in Detail the types of Personal Information" shared with each third-party entity. Appendix A, Specification No. 15. However, some Companies altogether failed to identify the types of Personal Information shared, while others provided broad categorizations that failed to actually identify any type of Personal Information. As a result, this report cannot provide generalized findings on the types of Personal Information shared. The FTC can state, however, that the types of Personal Information shared with third-party entities varied widely across the Companies (at least for those that reported what Personal Information they shared) and was likely broader than what consumers would have expected.

generally make data sets broadly available if there was a purported public interest in making such information more broadly available.

5. The Companies Generally Implemented Some Restrictions Governing Sharing with Outside Third Parties, But Had Fewer Restrictions Governing Disclosure to Corporate Affiliates

The Companies' internal disclosures, or the sharing of information with affiliates or corporate-branded entities, was most often governed by internal policies and the Companies did not require additional agreements or contracts. With respect to the sharing of information outside the Companies' corporate entities, the Companies often referred to the use of standard contractual language applicable to such sharing and disclosures. The use of such template contractual language, which was not tailored language to the unique circumstances of individual sharing arrangements, may not be sufficient to protect consumers' privacy and security. In addition, no Company described any audit or other ongoing diligence to ensure that those entities receiving the information were complying with any governing use restrictions in its contracts or terms of service. Rather, many Companies appeared to rely on the existence of such agreements to meet their data privacy obligations.

- **Affiliates or Company-Branded Entities**: With respect to the use restrictions in place to govern sharing with affiliates or other corporate-branded entities, most Companies reported that their own existing consumer-facing privacy policies or internal policies and procedures governed such data disclosures. Very few Companies reported having a specific approval process or additional contractual language with affiliates that governed disclosure. This lack of comprehensive approval processes or contractual language is concerning, especially where Companies reported having corporate entities incorporated in foreign jurisdictions like China, the United Arab Emirates, and Ukraine, or where acquisitions have substantially increased the size and breadth of a Company's data sharing or decreased the existence of providers with alternative policies.

- **Third Parties**: With respect to restrictions implemented to govern data sharing with third parties, most Companies reported that they needed to have contracts with third parties prior to any sharing.[142] Of the contracts provided that governed the Companies' relationships with service providers/vendors, there were several contractual provisions that appeared in multiple Companies' contracts (though not all contracts contained all provisions): the requirement that the service provider/vendor only use the Company's data for the purpose for which it was provided; that the service provider/vendor implement reasonable safeguards to protect the data provided; and that the service provider/vendor notify the Company of a breach or other unauthorized access to the data. Some contracts referenced various laws and regulations, such as the

[142] Some Companies produced representative contracts or data protection addendums, but no Company involved in the sharing of consumers' Personal Information produced contracts that governed all of their data sharing and in every instance.

CCPA,[143] the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[144] the European Union's General Data Protection Regulation ("GDPR"),[145] and the Payment Card Industry standards,[146] and explicitly required service providers/vendors to comply with such laws and standards.

Beyond contracts, some Companies reported that their existing policies (including privacy policies) applied to such sharing, even if the third-party recipient had not contractually agreed to such language. For example, several Companies had policies or legal terms that applied to developers. Some of the most common policy provisions that applied to such relationships were as follows: developers could not sell any data obtained from Companies; the developers needed to implement reasonable safeguards to protect the data; developers needed only to retain the data as long as necessary to fulfill the purpose for which the Company shared it; and developers needed to notify the Company of any unauthorized access to data. Most Companies did not have a formal internal vetting and approval process that all third parties must have undergone before sharing consumers' Personal Information with them.

- **Researchers and Academics:** With respect to the contracts or policies that applied to the Company SMVSSs that shared information with academics or researchers, most required academics/researchers to submit proposals or to sign contracts with the Company. Most of these Companies had contractual language that was specific to academics/researchers. Common contractual provisions in the agreements specific to academics/researchers included: requirements to use reasonable safeguards to protect data; restrictions to use the data only for the stated research project/purpose; and prohibitions against disclosure of data to a third party without the Company's written permission.

  The other Companies that shared information with academics/researchers did not appear to require any formal contract specific to academics/researchers. Instead, they required academics/researchers to comply with various policies for developers. With respect to the developer policies that were reused for academics/researchers, a common provision was: the researcher/academic needed to use reasonable safeguards to protect data.

  For at least one Company, the use restrictions differed based on how the academics/researchers were accessing the data—for access of information via the API, the academics/researchers had to

[143] Cal. Civ. Code § 1798.100 et seq..

[144] Public Law 104-191.

[145] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) (hereinafter "General Data Protection Regulation").

[146] Jennifer Simonson & Rob Watts, *What Is PCI Compliance? Everything You Need to Know*, FORBES (Aug. 10, 2022), https://www.forbes.com/advisor/business/what-is-pci-compliance/.

sign a contract, but for access to the SMVSS's publicly available data sets, they needed only to agree to the SMVSS's policies.

B. Data Minimization, Retention, and Deletion

1. Data Minimization Efforts Varied and Did Not Always Match Stated Principles

Data minimization generally refers to the practice of limiting the collection, use, disclosure, and retention of data to only what is necessary.[147] Even though the Companies' business models incentivized collecting as much data to monetize, they all reported engaging in, and implementing, data minimization principles, though the specific principles differed across the Companies. Common data minimization principles enumerated by the Companies included: collecting a minimal amount of Personal Information from users; collecting only data that is needed for a specific business purpose or need; retaining data only as long as it is needed for a business purpose; and processing data only for a limited and specific purpose. Less common data minimization principles enumerated by the Companies included: deleting or deidentifying data when the Company no longer needed it; providing users with controls to limit data processing; and using anonymized or pseudonymized data when possible. This demonstrates that, while all the Companies stated that they adhered to data minimization principles, their responses referenced varying degrees of data minimization efforts, and the resulting practices and procedures varied widely.[148] Moreover, the data minimization policies referenced by the Companies

---

[147] *See, e.g.*, FED. TRADE COMM'N, Bringing Dark Patterns to Light (Sept. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf (stating "[b]usinesses should collect the data necessary to provide the service the consumer requested, and nothing more."); FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (stating "[d]ata minimization refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it."). *See also United States v. Edmodo, LLC*, No. 3:23-cv-02495-TSH (N.D. Cal. June 27, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3129-edmodo-llc-us-v (Provision III of Order prohibits Defendant from "[c]ollecting more [p]ersonal [i]nformation than reasonably necessary for the [c]hild to participate in any activity offered on any such website or online service."); *Chegg, Inc.* (Provision V of the final Order requires that Respondent design, implement, and maintain "[p]olicies and procedures to minimize data collection, storage, and retention . . . ."); Drizly, LLC, No. C-4780 (F.T.C. Jan. 10, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023185-drizly-llc-matter (Provision III of the final Order requires that the Corporate Respondent document a public data retention schedule, including data minimization principles such as: "(1) the purpose or purposes for which each type of Covered Information is collected; (2) the specific business needs for retaining each type of Covered Information; and (3) a set timeframe for Deletion of each type of Covered Information that precludes indefinite retention of any Covered Information . . . ."); Residual Pumpkin Entity, LLC, No. C-4768 (F.T.C. June 24, 2022), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter (Provision II of the final Order requires that Respondents design, implement, and maintain safeguards to "minimize data collection, storage, and retention . . . .").

[148] For example, some Companies truly appeared to limit their data collection to what was necessary to operate the SMVSS. Other Companies appeared willing to collect any and all types of data, as long as there was an alleged business need or purpose that could support such collection.

were often vague or undocumented,[149] which may not be sufficient to protect against privacy and security risks, and to protect consumers from associated harms.

With respect to how the Companies ensured that employees complied with data minimization principles, they reported doing so through the following practices: training on data minimization principles; implementing data access controls; and requiring that employees comply with corporate data minimization policies (whether an individual data minimization policy or data minimization principles incorporated into other policies or codes of conduct). With respect to third parties with whom the Companies shared data, a majority of the Companies stated that they required the third parties to enter into contractual agreements with data minimization requirements. Several Companies required only some third parties to agree to the Companies' policies and agreements, without formally signing a contract. Less common means of ensuring that third parties complied with a Company's data minimization practices included the following: implementing technical controls to limit access to data; providing the third party with de-identified, aggregated, or hashed data; and maintaining direct oversight of the third party's practices. Some Companies reported that they enforced data minimization principles through privacy or data security review processes.[150]

2. Data Retention and Deletion Policies Varied Across the Companies

Data retention and deletion principles are a component of data minimization in that data should be retained only as long as there is a legitimate business need or to accomplish the purpose for which it was collected, at which point it is deleted.[151] All the Companies reported implementing data retention and deletion practices, and the majority reported having written data deletion and retention policies in place. Of those Companies that reported having written data deletion and retention policies in place, only about half produced actual written policies exclusively related to data retention and deletion. The other half produced a variety of policies that they said constituted their data retention and deletion policies. Such Companies produced privacy policies, law enforcement guidelines, and other written documents as evidence of their data retention and deletion policies. While these documents may have generally referred to some retention and deletion practices, they were vague and not comprehensive or exhaustive. This suggests that these Companies did not, in practice, have actual written data retention and deletion policies. A few Companies implicitly conceded that they did not have any comprehensive written data retention and deletion policies.

---

[149] Most Companies did not report having a specific written policy or procedure that included data minimization principles.

[150] Most of these privacy or data security reviews occurred when the Company was proposing a new/modified product or service that involved the collection of Personal Information from consumers, or prior to sharing user data with a third party.

[151] *See, e.g.*, FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS, https://www.ftc.gov/business-guidance/resources/start-security-guide-business (stating that businesses should "[h]old on to information only as long as you have a legitimate business need."); Blackbaud, Inc., No C-4804 (F.T.C. May 20, 2024) (Provision II of Decision and Order stating that Respondent must make available and adhere to a data retention schedule that sets forth, among other things, the purpose for which information is maintained, and the specific business needs for the retention of such information); *InMarket* (Provision X of Decision and Order stating that Respondent must make available a data retention schedule that sets forth, among other things, the business purpose for which information is collected and used, and the specific business purpose for retaining each type of information).

Regardless of whether a Company had a formal written data retention and deletion policy in place, all Companies stated that they followed at least some data retention and deletion practices with respect to users' Personal Information. The data retention and deletion practices varied across the Companies. Collecting Personal Information from Children did not necessarily spur the Companies to adopt stricter data retention and deletion practices, despite their COPPA Rule obligations.[152] With respect to retention periods, the Companies reported retaining data for as long as there was a business purpose; until the user actively deleted the data; or after a set period of time.[153] Retaining data for as long as there is a supposed business purpose, without additional information or specificity, may result in indefinite retention as it has no concrete end date.[154] All of the Companies noted that there were exceptions to their data retention and deletion practices, most often for legal, security, or tax and accounting purposes.[155]

Only a few Companies reported automatically deleting inactive or abandoned user accounts.[156] Some Companies would provide the user with notice in advance of deletion, but others did not. A few Companies reported that they would not delete inactive or abandoned accounts, instead retaining such accounts until the account user actively chose to delete the account.[157] Generally speaking, most Companies did not proactively delete inactive or abandoned accounts.

All Companies reported having procedures in place wherein they would delete accounts upon user request.[158] A few Companies also reported having processes wherein non-registered users could also submit a request to have their information deleted. Such capability is helpful, but not a failsafe in a world where content from various SMVSSs is shared with others outside of the platform, such as by text

---

[152] A few Companies reported more stringent data retention and deletion practices with respect to information collected from Children, but other Companies reported implementing the same data retention and deletion practices regardless of the age of user.

[153] Some Companies reported a mix of retention periods, with the applicable retention period depending on the type of Personal Information at issue.

[154] Retaining personal information collected online from a Child for as long as there is a supposed business purpose would be at odds with the COPPA Rule's requirement that a covered entity retain such personal information "only as long as is reasonably necessary to fulfill the purpose for which the information was collected." 16 C.F.R. § 312.10. *See, e.g.*, *United States v. Microsoft Corp.*, No. 2:23-cv-00836 (W.D. Wash. June 5, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923258-microsoft-corporation-us-v; *Amazon.com, Inc.*; *Edmodo, LLC*; *United States v. Kurbo, Inc.*, No. 22-CV-946 (N.D. Cal. Feb. 16, 2022), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923228-weight-watchersww; *Musical.ly, Inc.*

[155] A few Companies reported retaining certain data for research and development purposes.

[156] The length of inactivity prior to deletion varied by Company, generally anywhere from four to twelve months.

[157] One of the Companies reported to the Commission that it subsequently changed its practices to delete an account after it had been inactive for two years.

[158] *See infra* Section IV.C for more information regarding privacy rights afforded to consumers.

message, and an individual does not need to be a registered user to view content.[159] Also most Companies reported that, after receiving a user's deletion request, the Companies would do a "soft deletion" of the account. Soft deletion represents a period of time, usually between fourteen and ninety days, in which the user's data is not yet fully deleted.[160] At the end of this time, when the soft deletion period ended, the user's data is deleted. The purpose of the soft deletion period was to provide the user the opportunity to reactivate their account should they change their mind after submitting the deletion request. It appears that the soft deletion period also provided the Companies with more time to ensure that they deleted all data subject to the deletion request from the various databases and other environments where they could have stored the data, and that the Company stopped sharing the data with any third parties who had access to it.

Aside from user deletion requests, only a few Companies reported that they would consider third-party requests to delete user data. Such third-party requests were individually considered or related to instances in which a family member of a deceased user or the parent of a Child requested account deletion.[161] Again, all Companies noted that there were exceptions under which the Company would retain a user's data even after the user submitted a deletion request. Most commonly, the Companies reported retaining data subsequent to a user's deletion request for legal or trust and safety purposes. Some Companies noted that they would retain users' data, even after a deletion request, in some instances for business purposes.

The Companies' practices with respect to deletion (either upon user request or initiated by a Company) varied as well. A user would likely assume that deletion means that a Company would permanently erase their data. In fact, this understanding is not in line with several Companies' reported practices. For example, instead of permanently deleting data, some Companies instead reported de-identifying such data. These Companies claim that de-identification anonymized the data and removed any personally identifiable information. Even the Companies that reported permanently erasing user data nevertheless conceded that they did not delete all data submitted by a user, such as user-generated content that is public.

C. Consumer Rights Under GDPR

1. Rights Afforded Under the General Data Protection Regulation Were Not Automatically Afforded to American Consumers

In May 2018, the European Union's GDPR went into effect.[162] The European Union's "objective [with respect to] the GDPR was to give individuals more control over their personal data, and

---

[159] For example, some SMVSS content is viewable on a browser, outside of the SMVSS application itself. In such cases, the Company collected information from the viewer even if they were not a registered user of the SMVSS.

[160] Or otherwise de-identified or anonymized, as discussed later in this section.

[161] *See also* Section VII for more information regarding the Companies' practices with respect to Children. Most Companies reported that they would not delete a Teen user's account upon parental request.

[162] General Data Protection Regulation, *supra* note 145.

it goes about doing this by requiring . . . data privacy (ensuring people can exercise their right to privacy)."[163]

All of the Companies' SMVSSs operate both in the United States and Europe. As such, the Commission was interested in examining whether the Companies extended to American consumers the data privacy rights afforded to European consumers.[164] Only a few Companies reported that they extended to U.S. users the same protections they provided to European users under the GDPR. Most Companies stated that some but not all of the changes that they made in response to the GDPR they also extended to U.S. users.

Among other requirements, Chapter 3 of the GDPR includes consumers' data privacy rights, such as a consumer's right to access their personal information, the right to request that data be deleted or corrected for accuracy, and the right to be able to transfer one's data (i.e., "port" their data) to a third party of one's choice (where technically feasible).[165] Such data privacy rights are not uniformly available to U.S. users.

- **Access**: The "right of access by the data subject"[166] asserts, in part, that users "have a right to be provided with the personal data[167] of theirs that [the data controller[168]/data processor[169] is] processing."[170] All Companies reported enabling U.S. users to access their data collected by the SMVSSs. The Companies utilized various methods to implement the access request process, including the following: compiling a report containing the user's data and sending the report to the user; or providing an interface on the SMVSS where a user can either see the data collected

---

[163] *Do consumers know their GDPR data privacy rights?*, GDPR.EU, https://gdpr.eu/consumers-gdpr-data-privacy-rights/#:~:text=The%20objective%20of%20the%20GDPR,exercise%20their%20right%20to%20privacy.

[164] *See* Appendix A, Specification No. 52.

[165] General Data Protection Regulation, *supra* note 145, at chapter III.

[166] *Id.* at art. 15. The GDPR defines a "data subject" as "an identified or identifiable natural person." *Id.* at art. 4(1).

[167] The GDPR defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." *Id*. at art. 4(1).

[168] A data controller is "[t]he person who decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you." *What is GDPR, the EU's new data protection law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/#:~:text=The%20regulation%20was%20put%20into,tens%20of%20millions%20of%20euros.

[169] A data processor is "[a] third party that processes personal data on behalf of a data controller . . . ." *Id.*

[170] *A guide to GDPR data privacy requirements*, GDPR.EU, https://gdpr.eu/data-privacy/. The right of access also affords data subjects the right to obtain information regarding "the existence of automated decision-making, including profiling . . . meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject." General Data Protection Regulation, *supra* note 145, at art. 15.

about them or be directed to locations on the platform where they can access their data. Most Companies also reported having a process to provide access to data, pursuant to a parent or legal guardian's request, from a Child user's account.[171]

- **Deletion**:[172] The "right to erasure ('right to be forgotten')"[173] asserts that "data subjects have the right to request that [the data processor] delete any information about them that [the data processor has]."[174] Most Companies reported enabling U.S. users to delete their data collected by the SMVSSs.

- **Accuracy**: The "right to rectification"[175] asserts that "people have a right to correct inaccurate or incomplete personal data that [the data processor is] processing."[176] Very few Companies reported explicitly enabling U.S. users to correct their data for accuracy.[177] The Companies that offered U.S. users the ability to correct or modify their data did so through interfaces on the SMVSS.

- **Porting**: The "right to data portability"[178] requires that data processors "store [their] users' personal data in a format that can be easily shared with others and understood."[179] Most Companies reported providing U.S. users with a means to request their data in a format that the user could port, or transfer, to another platform. The Companies provided users with an interface on the SMVSS to request the user's data, but the format of the subsequent report differed across the Companies.[180] With various report formats, the actual ability of users to port their data to another SMVSS is unclear.

---

[171] Sometimes, this process would ultimately result in the Company disabling the account and deleting any data collected.

[172] *See supra* Section IV.B.2 for information on how the Companies implemented the data deletion process.

[173] General Data Protection Regulation, *supra* note 145, at art. 17.

[174] *Supra* note 170.

[175] General Data Protection Regulation, *supra* note 145, at art. 16.

[176] *Supra* note 170.

[177] While many Companies reported that users could access their SMVSS settings or profiles to update or delete data, staff sees this as being distinct from providing users with the means to update or correct the accuracy of all data held by a Company, especially since the Companies had much more data about consumers than what consumers proactively provided in a consumer-facing interface.

[178] General Data Protection Regulation, *supra* note 145, at art. 20.

[179] *Supra* note 170.

[180] The data reports delivered to users subsequent to such requests came in CSV, JSON, or HTML formats.

Despite generally having vast amounts of information on consumers' user experiences when it comes to advertising and User Engagement, about half of the Companies did not do any testing to ensure that consumers could exercise these privacy choices. The other Companies did not do any analyses or testing of user interfaces during the time period in question and made no substantive changes to the interfaces. It is surprising that half of the Companies did not analyze or test such user interfaces, especially since the time period in question covered the year following the implementation of the GDPR (2019) and the year when the CCPA went into effect (2020).

D. Key Findings

This section makes the following key findings, although each finding may not be applicable to every one of the Companies in every instance.

- **Companies failed to adequately police their data handling.** The unwillingness or inability of many Companies to specifically articulate to the Commission the breadth of their data collection from various sources, their lackluster or nonexistent written policies, and their broad sharing with affiliates or third parties raise serious concerns regarding the adequacy of their data handling controls and oversight. Many companies' insistence that their data collection practices are justified simply because they are "disclosed" to consumers only amplifies such concern. These so-called disclosures are very hard to read (often made across various policies, located in different places across websites, apps, etc.), nearly impossible to understand, too vague to effectively communicate a platform's actual practices, and subject to change (and it is up to the consumer to determine what has changed and when).

- **Companies are in the best position to implement privacy protective measures—but they often did not.** The Companies are in the best position to implement policies and practices to protect their consumers' privacy, but, to varying degrees, they did not do so. Indeed, there is an inherent tension between business models that rely on the collection of user data and the protection of user privacy. Many of the privacy-promoting practices implemented by the Companies are the result of state or international privacy regulations. Until a law requires SMVSSs to implement strong privacy practices, many Companies (and likely some other SMVSSs) may continue to present a pretense of privacy-focused practices while collecting and using as much data as possible in ways that result in financial returns for the corporate entity at the expense of consumers' privacy.

- **Companies' reported practices did not consistently make consumers' privacy a priority.**[181]

[181] *See, e.g.*, Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RES. CTR (Nov. 15. 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

- **Data Collection:** As described in this report, many Companies collected data about consumers from numerous sources, including from sources beyond the consumer themselves. This is especially concerning where some of the Companies appeared incapable of comprehensively relaying what consumer information they collected or used.[182]

- **Data Sharing with Affiliates or Company-Branded Entities:** Most of the Companies reported sharing consumers' Personal Information with affiliates or company-branded entities. Many SMVSSs are part of extensive corporate conglomerates—including those active in foreign countries—that provide a multitude of products and services beyond SMVSSs. One could imagine that data from an SMVSS user could be used for vast (and perhaps unknown) purposes beyond that which it was collected for, such as AI training.

- **Data Sharing with Third Parties:** Most of the Companies shared consumer information with third parties, and several were incapable of or unwilling to identify all instances (including the name of the third party) in which the Company shared consumers' Personal Information and the purpose behind such sharing.

- **Data Minimization:** While all of the Companies reported implementing data minimization principles, very few had actual written data minimization policies. Without a written policy that employees can reference and that the public can review, the Companies cannot ensure that data minimization will occur in practice or be held accountable when they fail to live up to their data minimization principles.

- **Data Retention:** Our review found that few Companies had transparent and specific data retention policies (e.g., a specific retention period for a piece of consumer data). The promise to retain data only as long as there is a "business purpose" is illusory—without specific and clear restrictions on what constitutes such a purpose, Companies can use a vague policy to indefinitely retain consumer data without any intent to ever delete it. The Companies were unclear on what would constitute a "business purpose." This terminology is open-ended and provides no clarity on a Company's practices. And, with the ever-increasing presence of AI, Companies may argue that training AI models is a "business purpose" that justifies retaining consumer data indefinitely.

- **Data Deletion:** When data was no longer needed, several Companies anonymized, pseudonymized, deidentified, or aggregated data instead of deleting the data altogether. There is research demonstrating that such data can nevertheless be re-

[182] *See, e.g.*, *supra* Section IV.A.1 for a discussion regarding User Attributes.

identified, suggesting that there is not a real substitute to deletion and retaining even purportedly deidentified data carries risks.[183]

- **Privacy Policies:** SMVSSs' privacy notices can frequently be lengthy, vague, and generally unhelpful. In their responses to the Order, the Companies often cited to numerous different privacy policies, terms of service, terms of use, and other consumer-facing legal documents as evidence of their practices. However, Commission staff was often unable to decipher such policies and notices and clearly ascertain the Companies' actual practices. If attorneys and technologists with privacy expertise cannot clearly and with certainty determine an SMVSS's practices from such policies, it is unclear how the average consumer would be able to understand them. This leaves consumers incapable of genuinely understanding what data SMVSSs collected from or about them, or how SMVVSs used that information. In these circumstances, the notice provided to consumers is illusory, and consumers cannot truly make a choice.

V. Advertising Practices

Advertising, and, in particular, targeted advertising powers the business model of many of the Companies and accounts for most of their revenue. Under this approach, certain Companies offered advertisers precise targeting of ads to users who exhibited specific characteristics and met defined criteria. This targeting was achieved through the collection of enormous volumes of user data gathered in a multitude of ways, as previously discussed.[184] Many of the practices discussed in this report stem from this business model, which create incentives to increase engagement that, in turn, facilitates the vast data collection upon which targeted advertising relies.

Targeted advertising involves the tracking of consumers' online activities in order to deliver tailored advertising. As previously discussed, SMVSSs have access to massive troves of data from or about users, including information inputted directly by users (e.g., profile information), information gleaned from user actions taken on and off SMVSSs, and even, in some cases, offline data from data brokers and others. This data was fed into detailed user profiles, which SMVSSs made available so advertisers could target specific groups of users who were more likely to be interested in the product or service being advertised. The mechanics of how an advertisement gets targeted and served to a user involved an incredibly complex set of interactions between the SMVSS, an advertiser, and in some cases, other third parties. An example of how an ad is targeted to a user is shown in the following example and related graphic:

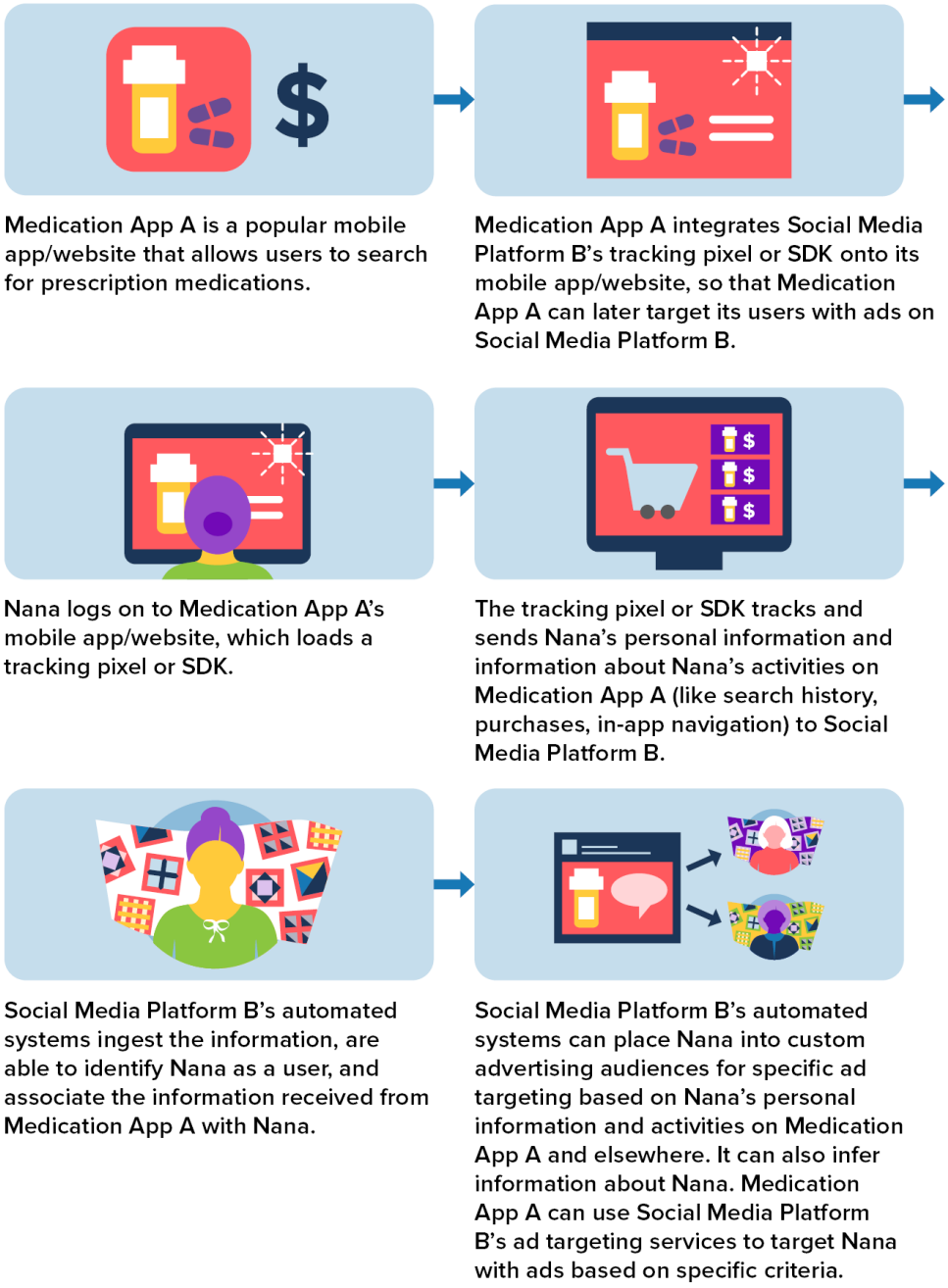
---

[183] Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 GEO. L. TECH. REV. 202 (2017), https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/#:~:text=If%20a%20data%20set%20is,re%2Didentify%20the%20individual%20involved (stating that "scrubbed data can now be traced back to the individual user to whom it relates").

[184] *See supra* Section IV.A for information regarding the Companies' data collection, use, and disclosure practices.

Example: *Medication App A is a popular mobile app that allows users to search for prescription medications. It uses social media platform B's advertising services to advertise its products. Medication App A integrates social media platform B's pixel or SDK onto its website or mobile app. A Medication App A user uses the app, and information about them and their activities are transferred to social media platform B, so that Medication App A can target ads to its users on social media platform B.*

Example of How a Company Could Use
a Person's Activities Off the Platform for Targeted Advertising



In this section, we describe the targeting capabilities that the Companies offered to advertiser customers, including notable similarities and differences. As part of this discussion, we summarize advertising restrictions regarding sensitive categories and Children and Teens that these SMVSSs claimed to use. Next, we outline the privacy-invasive tracking technologies made available by some of the Companies to facilitate tracking and targeting of users. We conclude by offering key take-aways regarding the Companies' targeting practices.

A. Targeted Advertising Poses Privacy Risks to Consumers

Targeted advertising can pose serious privacy risks to consumers.[185] It is far from clear that users know the extent to which they are being tracked when they engage with a given SMVSS; it is even more unlikely that consumers know that even their activity *off* of many SMVSS may be automatically collected and shared with the SMVSS. Many users may not know that the information they input directly (e.g., birthdate, home address) may be used for advertising, and the extent to which their every click, search, and action is being collected, logged, saved, and, in some cases, shared, including their activity off of the SMVSS. The data collected using the tracking technologies described below can be invisible to users. Consumers are frequently unaware of the potential downstream uses—including the sale to third parties of location data that may be used to identify consumers and their visits to sensitive locations, such as houses of worship and doctors' offices—of the immense amounts of data collected about them.[186]

In recent survey data, consumers expressed strong concerns about the use of certain categories of information for ad targeting. For example, according to a 2021 study, 73% of consumers were opposed to companies tracking online behavior and collecting personal data in order to serve targeted ads.[187] This same study revealed that 56% of consumers surveyed were opposed to companies displaying ads based on age, gender, and general location.[188]

---

[185] Although this report focuses on privacy risks to consumers from targeted advertising, such targeting also poses other risks to consumers, including increased fraud, systemic risk from data breaches, and potential exclusion from economic opportunities.

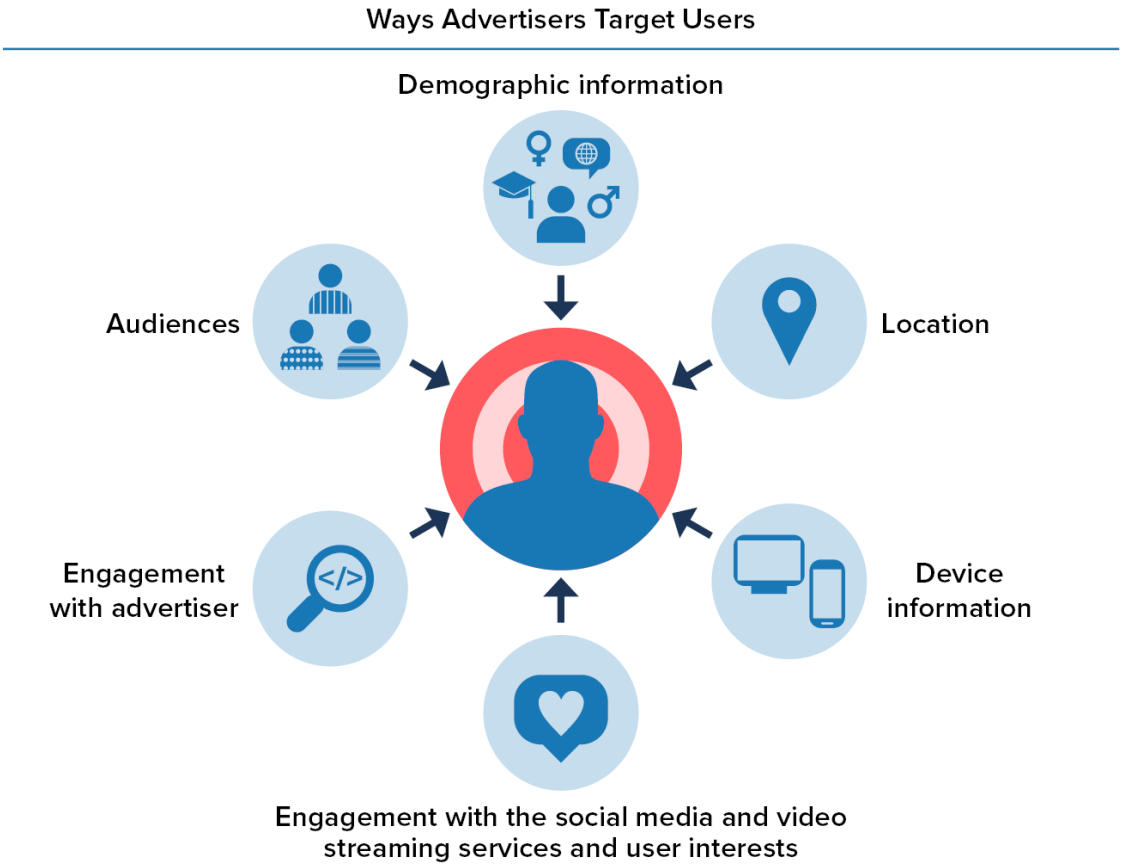
[186] *See, e.g.*, Amended Complaint for Permanent Injunction and Other Relief, *Fed. Trade Comm'n v. Kochava, Inc.*, 2:22-cv-00377-DCN (D. Idaho filed June 5, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/26AmendedComplaint%28unsealed%29.pdf ("Indeed, once information is collected about consumers from their mobile devices or other sources, the information can be and, in many instances, is provided multiple times to companies that consumers have never heard of and never interacted with. Consumers have no insight into how this data is used – they do not, for example, typically know or understand that the information collected about them can be used to track and map their past movements and that inferences about them and their behaviors will be drawn from this information."); *X-Mode Social, Inc*.

[187] *Accountable Tech: Frequency Questionnaire*, GREENBERG QUINLAN ROSNER (Jan. 28-31, 2021), https://accountabletech.org/wp-content/uploads/Accountable-Tech-013121-FQ-Methodology.pdf.

[188] *Id.*

B. Targeting Capabilities

1. Targeting Similarities and Differences



We found certain similarities in the targeting capabilities offered by several Companies to advertisers. We observed that the Companies with SMVSSs that offered a Digital Advertising Service[189] generally offered advertisers the option to target users based on some or all of the following:

- **Demographic Information:**[190] Many Companies offered advertisers the ability to target users with ads based on Demographic Information, including, for example, age range (e.g., ages 18-22), gender (e.g., female), education (e.g., college-educated), and language (e.g., English). In some cases, this Demographic Information was input directly by SMVSS users, and in other cases it was inferred by the Company. As described below, some Companies reported that there

[189] *See supra* Section III for more information on the Companies and Digital Advertising Services.

[190] *See supra* note 95.

were limitations on such targeting and that they had policies prohibiting targeted ads relating to certain sensitive categories, such as political affiliation or sexual orientation.

- **Location:** Many Companies offered advertisers the ability to select the geographical location where they would like their ads to run on their SMVSSs. Location could have been based on the consumer's stated location, IP address, device SIM card, or other mobile location data. This information was used to target ads to users in specific locations.

- **Device Information:** Some Companies offered advertisers the ability to target ads to their SMVSS users based on the characteristics of the device the consumer was using, including operating system, device type, device model, device price, and carrier.

- **Engagement with the SMVSS and User Interests:** Some Companies received data on specific user activity and behavior on the SMVSS. As users engaged with the SMVSSs, the SMVSSs learned more about user habits and may have targeted ads to users based on the habits the Company could observe and analyze. For example, this engagement data enabled an advertiser to target ads to users who indicated that they liked the advertiser's page on the SMVSS. Further, SMVSSs offered advertisers the ability to target ads to users based on interests inferred from a consumer's actions within the SMVSS, and, in some cases, other information. These SMVSSs assigned users to interest categories based on their SMVSS activity. For example, if a user routinely engaged with recipes (e.g., read recipes or posted recipes), the user may have been added to the "Food and Drink" interest category and targeted with food and drink ads.

- **Engagement Off SMVSS with Advertiser:** Some Companies also received from advertisers information about user behaviors and actions that the user took on the advertiser's website or app, or customer data that the SMVSSs used to facilitate targeting. These Companies offered advertisers small pieces of code that the advertiser could integrate into its website or app. This code enabled the Companies to receive detailed, granular information about the actions and behaviors of users on the advertiser's site. Other advertisers supplied the Companies with customer information, often hashed and consisting of contact lists, email identifiers and other identifiers that an advertiser obtained from its customers. The information supplied by advertisers to the Companies regarding User Engagement off of the SMVSS was frequently used to create the audiences described below.

- **Audiences:** Several Companies offered advertisers the ability to target ads to what is commonly referred to as custom audiences[191] and lookalike audiences.[192] As described in further detail below, these Companies often made available privacy-invasive tracking technologies to allow advertisers to carry out this form of targeting.

Although we observed similarities in the way the Companies targeted users, we also observed some outlying practices. For example:

- At least one Company did not target ads to individual users, and instead served ads that were contextual, rather than targeted, in nature.[193] Other companies did not appear to do this, however.

- A few Companies imported third party data sets that included location and age information from data brokers and others, as a way of providing advertisers with additional information about users for ad targeting. This information was imported into the ad targeting platform and available to advertisers to target ads. In some cases, the third parties that provided the information received a percentage of advertising revenue that the Company received when advertisers used these data sets.

- A few Companies inferred information about users, such as age and gender, through machine learning.

- We observed only one Company that allowed users to download data to see how they had been categorized for ad targeting purposes.

C. Targeting Based on Sensitive Categories

Although most of the Companies in this study engaged in targeted advertising using the methods described above, most claimed to prohibit targeting users based on sensitive categories (such as political affiliation, race, religion, health, or sexual orientation) and represented that they had restrictions in place regarding ads targeted at Children and Teens.

---

[191] A custom audience is a group of users that are part of an advertiser's marketing list or that have engaged with the advertiser's advertisements, apps, or website.

[192] Through lookalike audiences, advertisers attempt to target users who share similar attributes with the advertiser's existing customers.

[193] *See supra* note 93 discussing contextual advertising.

1. Profound Threats to Users Can Occur When Targeting Occurs Based on Sensitive Categories

Targeted advertising based on sensitive categories can be extremely harmful to consumers and cause a wide range of injuries to users.[194] These injuries run a wide spectrum and include, for example, unlawful discrimination, emotional distress, stigma, reputational harm, embarrassment, and invasion of privacy.[195] Targeted ads based on knowledge about protected categories can be especially distressing. One example is when someone has not disclosed their sexual orientation publicly, but an ad assumes their sexual orientation. Another example is when a retailer identifies someone as pregnant and targets ads for baby products before others, including family, even know about the pregnancy.[196] These types of assumptions and inferences upon which targeted advertising is based can in some instances result in emotional distress, lead to individuals being misidentified or misclassified, and cause other harms.[197]

Many of the Companies claimed in their policies to prohibit targeting based on sensitive categories, such as race, religion, sexual orientation, and political affiliation. There was, however, an overall lack of consistency about which categories were considered sensitive and how the Companies described these prohibited forms of targeting in their policies. This lack of clarity makes it challenging for consumers and other stakeholders to understand the precise contours of the prohibited practices. This could lead to uneven application of this prohibition and perhaps even instances where practices understood to be prohibited may occur.

---

[194] The Commission notes that targeting advertising based on categories that are not sensitive on their own but can be combined to produce proxies for sensitive categories can also result in consumer harm. *See* Dep't of Hous. & Urb. Dev. v. Facebook, Inc., FHEO No. 01-18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf; *see also* Tracy Jan & Elizabeth Dwoskin, *HUD Is Reviewing Twitter's and Google's Ad Practices As Part of Housing Discrimination Probe*, WASH. Post (Mar. 28, 2019), https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination/.

[195] *See, e.g., How Online Ads Discriminate: Unequal Harms of Online Advertising in Europe* 11–13, EUR. Digital Rts. (2021), https://edri.org/wp-content/uploads/2021/06/EDRi_Discrimination_Online.pdf; Rae Nudson, *When targeted ads feel a little too targeted*, VOX (Apr. 9, 2020), https://www.vox.com/the-goods/2020/4/9/21204425/targeted-ads-fertility-eating-disorder-coronavirus. *See also* Compl. ¶ 80, *GoodRx Holdings, Inc.* (noting that unauthorized disclosure of facts about consumers' health, including physical or mental health conditions, medical treatments, disability status, substance addiction, sexual and reproductive health, and sexual orientation is likely to cause them stigma, embarrassment, or emotional distress, and may also affect their ability to obtain or retain employment, housing, health insurance, disability insurance, or other services); *United States v. Easy Healthcare Corp.*, No. 1:23-cv-3107 Compl. ¶ 49 (N.D. Ill. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v (noting that unauthorized disclosure of facts about consumers' sexual and reproductive health is likely to cause them stigma, embarrassment, or emotional distress, and may also affect their ability to obtain or retain employment, housing, health insurance, disability insurance, or other services).

[196] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[197] *See How Online Ads Discriminate: Unequal Harms of Online Advertising in Europe*, *supra* note 195, at 12.

2. Children and Teens

Children and Teens spend a significant amount of time online. A recent survey found that 88% of teens between thirteen and eighteen have their own smartphone, and 57% of children between eight and twelve have their own tablet.[198] The more time Children and Teens spend online, the more likely they are to have their information collected and see ads. It is no surprise then, as previously noted, that the Companies reported studying and analyzing User Engagement to serve content, including advertising content, to users, as targeted advertising incentivizes engagement, which in turn incentivizes keeping Children and Teens online.[199] As digital media consumption increases, Children and Teens see more advertising and marketing messages. According to one estimate, some Teens may see as many as 1,260 ads per day.[200] Children and Teens may be lured through these ads into making purchases or handing over personal information and other data via dark patterns. The harms to Children and Teens from SMVSSs and the ads on SMVSSs have been widely reported and range from the promotion of products detrimental to Children and Teens to effects on mental health.[201] These harms are particularly difficult for Children and Teens to avoid because frequently the advertising content is blurred—i.e., blended into the surrounding content—which allows marketers to disguise advertising and the persuasive intent of that content.[202]

With respect to Children, most Companies stated that they prevented Children from creating accounts.[203] Of the few Companies that reported that Children could create an account, most of these either did not permit advertising to their Child users or prohibited targeted advertising. With respect to Teens, almost all of the Companies permitted Teens to create accounts. However, when it came to advertising, some Companies reported distinct advertising practices with respect to Teens, such as limiting the types of ads that can be seen by Teens.

---

[198] *The Common Sense Census: Media Use by Tweens and Teens* 22, COMMON SENSE MEDIA (2021), https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf.

[199] *See* Section IV.A.3 for more information regarding how the Companies used consumer data.

[200] *See Kids for Sale: Online Advertising & the Manipulation of Children* 10, GLOB. ACTION PLAN (2020), https://www.globalactionplan.org.uk/files/kids_for_sale.pdf.

[201] *See id.* at 11-12; *see also infra* Section VII, notes 267-269, for more information regarding the potential harms to Children and Teens.

[202] FTC Staff Perspective, *Protecting Kids from Stealth Advertising in Digital Media* (Sept. 2023) at 4, https://www.ftc.gov/system/files/ftc_gov/pdf/p214505kidsadvertisingstaffperspective092023.pdf.

[203] As discussed in further detail in Section VII.D below, it is widely known that some Children circumvent the SMVVSS' age gates, effectively resulting in those Children likely viewing ads unrestricted.

D. Privacy-Invasive Tracking Technologies

Companies also reported the use of tracking technologies such as pixels,[204] SDKs,[205] or certain advertising APIs[206] to facilitate advertising to users.

As users interacted with websites and mobile apps, the technologies made available by some Companies were tracking users' online activities and gathering personal data about them. For example, these tracking technologies transmitted personal data such as how a user interacted with a web page or app, including specific items a user purchased, search terms the user entered, or information a user typed into a form on the page or app.

Much of this type of tracking occurs behind the scenes, with users unaware and unable to avoid what's happening. The nature of many of the data points that these technologies can gather, often without consumers' knowledge or consent—for example, health conditions, searches on sensitive websites, and responses to questionnaire—can be uniquely confidential. The use of these tracking technologies for advertising has drawn considerable scrutiny in media reports and research, and even led to legal actions.[207] The FTC has brought enforcement actions against advertisers relating to their use of SMVSS ad tech to target users with advertisements. For example, in *United States v. GoodRx*, the FTC alleged that tracking pixels made available by a Company allowed GoodRx to share personal health information, such as particular medications purchased by users and health conditions, with SMVSSs so GoodRx could target these users with health-related advertisements.[208] Similarly, in *United States v. Easy Healthcare*, the FTC alleged that an SDK offered by a Company's corporate parent allowed the developer of a pregnancy and fertility app to transmit the identifiable health information (including

---

[204] A pixel is a small piece of code that is inserted into a website or ad and configured to accomplish certain objectives (e.g., capture pageviews, clicks, interactions with ads). *See, e.g.*, Fed. Trade Comm'n Off. of Tech., *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking* (Mar. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.

[205] App developers integrate SDKs into their apps in order to track and analyze users' interactions with the app and this data is then transferred to the entity that made the SDK available. *See Easy Healthcare Corp*.

[206] *See supra* note 126.

[207] Press Release, Fed. Trade Comm'n, *FTC Warns Tax Preparation Companies About Misuse of Consumer Data* (Sept. 18, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-warns-tax-preparation-companies-about-misuse-consumer-data; *Easy Healthcare Corp.*; *BetterHelp, Inc.*, No. C-4796 (F.T.C. July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; *GoodRx Holdings, Inc.*; *Flo Health Inc.*, No. C-4747 (F.T.C. June 22, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc; Todd Feathers et al., *Out of Control: Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, THE MARKUP (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies; Mingjia Huo et al., *All Eyes on Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems*, PROC. OF THE 21ST WORKSHOP ON PRIVACY IN THE ELEC. SOC'Y (Nov. 7, 2022), https://dl.acm.org/doi/10.1145/3559613.3563190.

[208] *See GoodRx Holdings, Inc*.

information about users' fertility and pregnancies) of users of the app to the Company's parent for advertising purposes without providing users notice or obtaining users' affirmative express consent.[209]

A few of the Companies in this study acknowledged using tracking pixels and SDKs in connection with their advertising practices. It appears that the Companies that utilized these technologies were doing so in connection with the creation of custom and lookalike audiences offered to advertisers. For example, when an advertiser was looking to create a custom audience on its website using an SMVSS's pixel, the advertiser would have embedded the pixel into its site. Once the pixel was present, the advertiser could create, for example, detailed parameters of users the advertiser wanted to target, including users who added specific products to their shopping cart or users who visited its website within the last thirty days and then advertised to that group of users using the SMVSS's advertising products. The use of these pixels and SDKs has the potential to lead to significant privacy invasions and harms, including the injurious practices described above.

E. Key Findings

This section makes the following key findings, although each finding may not be applicable to every one of the Companies in every instance. It bears emphasizing that the data collection and tracking practices described in the findings below likely will remain the status quo, as the Companies' business models are built on such practices.

- **The collection of personal data by many of the Companies subjected users to the risk of significant privacy invasions and other risks, including from ad targeting.** It is difficult to quantify the amount of data collected by the Companies about users of their services. This data gives many of the Companies deep insights into consumers, including users' behaviors, actions, location, preferences, and searches conducted. Depending on how this data is used, risks abound for users, including inaccuracies and biases that can result in detrimental effects for consumers. And, as previously discussed, there are a wide range of potential harms that consumers may experience when ad targeting occurs.[210]

- **Companies that deployed targeted advertising also extensively tracked their users.** Most of the Companies engaged in ad targeting also extensively recorded user activity and behaviors through the use of tracking technologies that facilitate the collection of user data.

- **The lack of transparency in the Companies' advertising ecosystem prevents users from being aware their data was being collected and packaged for ad targeting.** Because the advertising ecosystem is complex and occurs beneath the surface, it is challenging for users to decipher how the information collected about them by many of the Companies is used for ad targeting. This challenge is exacerbated by the fact that consumers' use of these services was conditioned on targeting and because opting out of such targeting was often

[209] *See Easy Healthcare Corp*.

[210] *See* Section V.C.1 for more information on the threats to users from targeted advertising using sensitive categories of information.

impenetrable or unavailable to consumers. The lack of transparency and lack of consumer awareness and understanding poses concerns and suggests users do not understand how much privacy they are giving up, largely to facilitate targeted advertising, when using the services of the Companies.

VI. Algorithms, Data Analytics, or AI

There has been an explosion in the use of automated decision-making technologies and AI in recent years, raising novel technological, ethical, and legal issues. Many companies rely on these automated technologies to perform key business functions. The Companies covered in this report are no exception. Their responses demonstrate the extent to which (perhaps unknown to consumers) the Companies rely on Algorithms, Data Analytics, or AI to carry out their business functions.

The Companies reported broad usage of Algorithms or Data Analytics,[211] including applying them to consumer Personal Information[212] and Demographic Information[213] in order to analyze, process, and infer information, and to automate decisions or outcomes that power their SMVSSs and the user and non-user experiences on the SMVSSs. The Order asked for a broad range of information relating to the Companies' use of Algorithms or Data Analytics, such as identifying whether they use data privacy, bias, or ethics-focused professionals to work on Algorithms or Data Analytics,[214] and asked that they describe: the application and uses of Algorithms or Data Analytics as applied to users' Personal Information or Demographic Information;[215] the ways in which the Companies address privacy, security, or ethics issues relating to Algorithms or Data Analytics applied to Personal Information;[216] how the Companies evaluate, monitor, and test the application of Algorithms or Data Analytics to Personal Information;[217] whether and how the Companies use Algorithms or Data Analytics for advertising;[218] whether and how they use Algorithms or Data Analytics to measure, promote, and

[211] *See supra* note 7.

[212] *See supra* note 94.

[213] *See supra* note 95.

[214] *See* Appendix A, Specification No. 9.

[215] *See* Appendix A, Specification No. 27.

[216] *See* Appendix A, Specification No. 28.

[217] *See* Appendix A, Specification Nos. 29, 30.

[218] *See* Appendix A, Specification No. 31.

research User Engagement;[219] and whether and how they use Algorithms or Data Analytics to predict Demographic Information about their users.[220]

The specification requests covered a range of automated technologies and, as some Companies acknowledged, encompassed the use of AI and machine learning technologies.[221] AI is an ambiguous term with many possible definitions, but it "often refers to a variety of technological tools and techniques that use computation to perform tasks such as predictions, decisions, or recommendations."[222] Machine learning, natural language processing, and other tools are usually considered branches, types, or applications of AI.[223] Similarly, this report may refer to "automated systems" or "automated tools" broadly to mean software and algorithmic processes, including AI, that are used to automate workflows and help people complete tasks or make decisions.[224] Some tools mentioned in this section may not necessarily be AI-powered, while others are.

In this section, we describe the different ways in which the Companies applied Algorithms, Data Analytics, or AI to Personal Information (i.e., inputting Personal Information into automated technologies), as well as their approaches to monitoring and testing those automated systems. We highlight the privacy concerns associated with applying Algorithms, Data Analytics, or AI to Personal Information. We also highlight other harms from these practices, including systems that prioritize showing certain forms of harmful content, such as dangerous online challenges, and negative mental health consequences for Children and Teens. We conclude with key findings.

A. The Companies Relied on Algorithms, Data Analytics, or AI to Carry Out Most Basic Functions and to Monetize Their Platforms

All of the Companies referenced using Algorithms, Data Analytics, or AI. Most used these technologies for a variety of decision-making functions that the Companies described as key to the functioning of their services at a large scale, including the SMVSSs directed to Children and those that

---

[219] *See* Appendix A, Specification No. 32.

[220] *See* Appendix A, Specification No. 40.

[221] Some of the Companies in their responses specifically acknowledged that they understood "Algorithms or Data Analytics" to encompass AI and machine learning.

[222] Michael Atleson, *Keep your AI claims in check*, FED. TRADE COMM'N (Feb. 27, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check.

[223] *See* FED. TRADE COMM'N, COMBATTING ONLINE HARMS THROUGH INNOVATIONS (June 16, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf.

[224] Joint Statement on Enforcement of Civil Rights, Fair Competition, Consumer Protection, and Equal Opportunity Laws in Automated Systems (Apr. 4, 2024), https://www.justice.gov/crt/media/1346821/dl?inline.

permit Teens to use their services. In some cases, the services directed to Children use Algorithms, Data Analytics, or AI in the same manner as the SMVSSs that are not directed to Children.

Nearly all Companies reported applying Algorithms, Data Analytics, or AI to Personal Information or Demographic Information in one fashion or another. The most commonly reported uses by the Companies were:

- for content recommendation, personalization, and search functionality, and to boost and measure User Engagement;[225]
- for content moderation purposes or in connection with safety and security efforts;
- to target and facilitate advertising;
- to infer information about users; and
- for other business purposes, such as to inform internal strategic business decisions or to conduct research.

Other notable uses included to assist with the deployment of special effects, or to assist with enabling language translations or accessibility features such as closed captioning.

Nearly all Companies reported applying these technologies to Personal Information they collected. Some reported using Algorithms, Data Analytics, or AI more expansively, while a few reported using these technologies for more limited purposes, such as an SMVSS that used them for security and integrity purposes only. But the majority of SMVSSs used Algorithms, Data Analytics, or AI for multiple purposes.

Some Companies stated that they used Classifiers[226] in their deployment of Algorithms, Data Analytics, or AI, and they used them for a variety of functions described above, including for serving content and advertising, for content moderation, to infer information (such as age or interests), and for security, anti-spam, and integrity purposes. These Classifiers were either regularly or continually retrained. At least one Company did not appear to use Classifiers, and instead employed a manual registration and annotation process for unlabeled or unstructured data.

Most of the Companies derived revenue from their application of Algorithms, Data Analytics, or AI to Personal Information, whether directly or indirectly (although a few Companies did not directly or fully respond regarding whether they derived revenue from these technologies). The majority of Companies acknowledged that they derived revenue from these technologies indirectly by using them to power or improve their products and services that generate revenue, such as their advertising services

---

[225] *See supra* note 13.

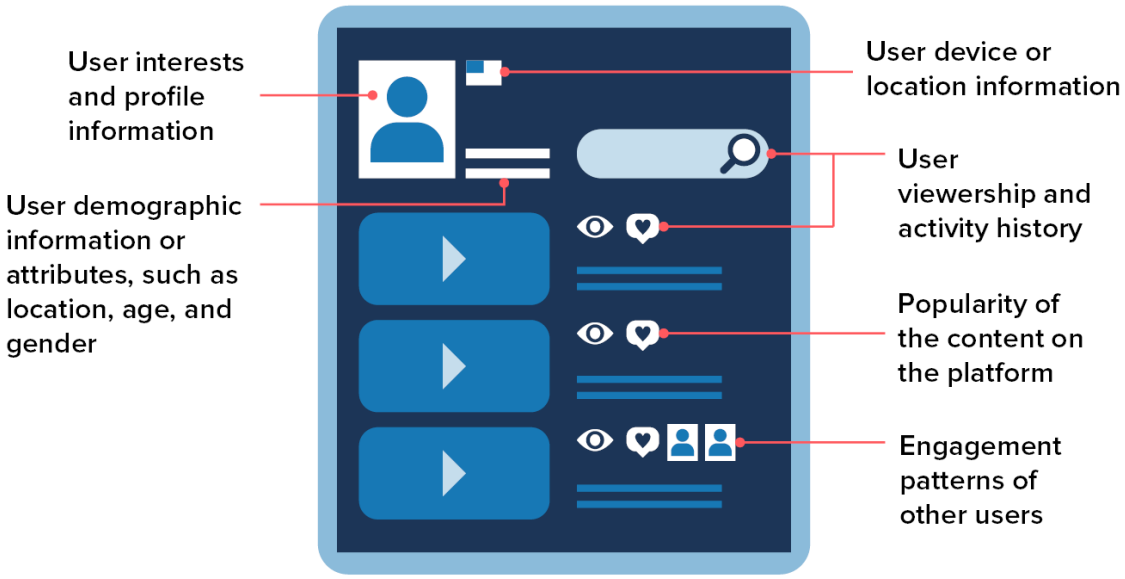
[226] The Order defines "Classifiers" as "a machine-based process that sorts unlabeled data into categories." Appendix A, Definition J.

(i.e., to serve ads) and their non-advertising products and services, such as access to premium subscription features. These Companies also acknowledged using these technologies to attempt to grow their user base, increase User Engagement, or improve products and the user experience, which also would lead to increased revenue. But at least one of the Companies in this study is part of a larger corporate structure that offers products and services unrelated to an SMVSS, leaving open the possibility that they use Personal Information, including Personal Information inferred by Algorithms, Data Analytics, or AI, or the outputs of those technologies, for those other products and services. Some Companies specifically noted that monetization was indirect, in that they did not monetize these tools through direct sales or sharing of data.

1. Content Recommendation, Search, and Boosting or Measuring User Engagement

Most Companies said they relied on Algorithms, Data Analytics, or AI for content personalization—to determine, based on users' information and activities, which content (such as user-generated pictures, videos, or other content) users were presented with, to recommend and present content in response to search queries, or to surface topics, content, and trends. These Companies described using a variety of technologies, such as Algorithms and machine learning models that worked to predict the probability that content is likely to be interesting or relevant to a particular user.

How the Companies Used the Automated Systems to Recommend Content to Users



In general, the Companies described complex algorithmic and machine learning models that looked at, weighed, or ranked a large number of data points, sometimes called "signals," that were intended to boost User Engagement and keep users on the platforms. These models predicted how likely a user was to be interested in or engage with content and ranked the order of the content presented. This includes content recommendation models that considered:

- user viewership and activity history, such as views or viewing history, search queries, replies or comments, the type of content a user interacted with and its popularity, time spent viewing content, or a user's interaction or feedback with the content ("likes" or sharing), click-through rate, or accounts, groups, pages, or content a user followed, and the content they posted;

- user interests and profile information;

- user device or location information;

- user Demographic Information or attributes, such as location, age, and gender, which may sometimes have been inferred by a Company based on other information;

- engagement patterns of other users, including engagement levels among users in similar demographic categories and cohorts, the actions that others were taking on the platform, such as friends, family, connections, and people with similar attributes or engagement; and

- the popularity of the content on the platform, such as the volume of views, comments, or the time other viewers may have spent watching content.

At least one Company explained that it looked at which content drove the most watch time and engagement for other viewers who made the same query.

Some Companies did not (or claimed they were unable to) identify factors that carried the most weight in recommending content (describing these models as complex, dynamic, and subject to change). Several Companies acknowledged that User Engagement and activity history (including of similar users) often were heavily weighted or carried the most weight in content recommendation Algorithms.

While the vast majority of SMVSSs stated that they used Algorithms, Data Analytics, or AI to personalize, promote, rank, and target content, a few SMVSSs stated that they did not rank, target, or promote content at all or did not do so using Algorithms, Data Analytics, or AI. For instance, rather than relying on Algorithms, Data Analytics, or AI, one SMVSS displayed content from other users in real time in the order in which it was posted. Internal documents of that Company state that because an Algorithm is not determining what a user sees, there was no endless scrolling or viral content on the platform.

Relatedly, another common use of Algorithms, Data Analytics, or AI was to measure User Engagement; some Companies generally described measuring user churn (i.e., customer attrition), performance and site visits, to measure a user's engagement with the platform or other users, or to provide analytics and other services to third parties.

2. Safety, Security, and Content Moderation

Companies reported using Algorithms, Data Analytics, or AI in their content moderation efforts, such as to detect and respond to reports of abuse, offensive material, or conduct that violated the Company's terms of use, service, or community guidelines. Some Companies with Child-directed SMVSSs reported using automated tools to moderate content and promote safety, and reported using

additional safeguards that applied only to Child users (such as the use of automated content filters, default settings that prevented the sending of links, or a stricter application of content moderation standards). At least one Child-directed SMVSS reported using automated filters to determine if content is "family-friendly," and therefore eligible for inclusion on the platform. At least one other SMVSS reported that its content moderation standards were applied more strictly as to what content could be displayed to Children, especially as to content that may have contained bullying, nudity or sexual content, graphic and violent content, and content celebrating crime. For instance, where an SMVSS might otherwise have displayed a graphic content warning for users thirteen and older, it would have removed such content altogether for Children. These SMVSSs reported relying on automated technologies or filters to identify such potentially violating content.

A number of Companies (including ones with Child-directed SMVSSs) reported using automated detection systems to detect, prevent, disable, or remove spam or abusive accounts, bots or other inauthentic traffic, fraudulent activity and transactions, platform manipulation, account compromise, or to detect illegal or objectionable content that violated the SMVSS's terms of use.

A few Companies stated that they had additional or differing content moderation policies for different types of accounts, such as those accounts held by journalists, artists, and documentary creators. For instance, at least one SMVSS reported that it permitted exceptions for content uploaded by such accounts that related to educational, scientific, documentary, artistic, or satirical content, content in fictional or professional settings, counter speech, or content that otherwise enabled individual expression on topics of social importance. Similarly, at least one Company stated that it allowed material that contained graphic content, if it was educational, scientific, newsworthy, or a documentary, and as long as the creator included relevant context to explain the content.

3. Inferring Personal and Demographic Information About Users and Non-Users

Most of the Companies reported that they used Algorithms, Data Analytics, or AI to infer information about individuals. At least one of the Companies reported using Algorithms, Data Analytics, or AI to infer information about users and non-users, including to infer Demographic Information. Some said they only inferred information about users and did not do so for non-users and their households.

Companies reported using inferred information for advertising, such as to create advertising audience segments, and for non-advertising purposes, such as inferred location, age, or gender to suggest content. Algorithms, Data Analytics, or AI were often used to infer characteristics and Demographic Information such as age and date of birth, gender, location, Familial Status[227] or Family

[227] The Order defines "Familial Status" as "the familial designation of a natural Person (e.g., spouse, Child, stepchild, parent, grandparent, parent-in-law, sibling-in-law, and child-in-law, among others)." Appendix A, Definition T.

Relationships,[228] as well as other categories such as language.[229] Some of the Companies appeared to have inferred other detailed categories of Demographic Information. This included data points such as: education level; relationship or marital status; parental status and age range of children (such as "New Parents," "Parents with toddlers," or "parents with teenagers"); household income percentile; locations visited; homeownership; employment; or industry. Some Companies referenced vague or broad categories, including categories described as "Employment; Household; and Other lifestyle details." At least one SMVSS inferred interests that could relate to Familial Status or Familial Relationships, and also could infer what appears to be Demographic Information based on data it received from third-party companies that created or supplied advertising audiences. Some Companies' responses were vague, so it was not clear what information was inferred rather than collected, and their responses left open the possibility that there were other inferred categories that were not reported. At least one SMVSS noted that it looked at a user's search history, viewing or watch history, and location information when inferring user information for advertising.

Some Child-directed SMVSSs also used Algorithms, Data Analytics, or AI to infer Demographic Information about their users. For instance, at least one Child-directed SMVSS said it inferred user gender, age, country, and region.

4. Advertising and Targeting

Some Companies reported applying Algorithms, Data Analytics, or AI, such as machine learning models, to Personal Information to target and serve advertisements (such as based on a user's specific interest or membership in a demographic-based category); to predict the likelihood that an advertisement would be relevant to a user and that a user would engage with it; to determine ad conversion; to place users into audience segments (such as based on specific interests or categories); or to develop custom and lookalike audience modeling.[230] At least one Child-directed SMVSS that did not allow personalized targeting, but did allow contextual advertising, made use of Algorithms, Data Analytics, or AI for contextual advertising purposes based on broad criteria (such as the user's country), and to decide which ad to contextually serve a user. Even Companies that did not have a Digital Advertising Service[231]

[228] The Order defines "Familial Relationship(s)" as "a description of the Familial Status of all members of a household (e.g., family of four with two parents and two Children)." Appendix A, Definition S.

[229] *See* Section IV for more information on the Companies' data practices.

[230] *See* Section V for more information on the Companies' advertising practices.

[231] *See supra* note 92.

made use of automated tools for their own advertising: for example, relying on a machine learning model to identify and target users likely to subscribe to a paid subscription of the SMVSS.

5. Other Purposes to Inform Their Business Strategy and Product Decisions

Other uses by one or more Companies included: to inform internal business decisions relating to the platform, such as informing investments relating to content and internal resources; to inform business decisions relating to new and existing products and services and user experience; to conduct research; to enable special effects and filters for video and content; for language translations and other accessibility features (such as closed captioning); and to "support and serve the public conversation." While some of these descriptions were vague, they underscore that Companies can monetize the application of Algorithms, Data Analytics, or AI to Personal Information in a variety of ways that likely are not known to users and non-users.

B. The Personal Information that Powers Algorithms, Data Analytics, or AI Came from Sources Including Offline Activity, Inferred Data, or Data from Third Parties

The Companies aggregated information about users (and some about non-users) from multiple places.[232] Some Companies reported less specificity than others about the categories of Personal Information they used for Algorithms, Data Analytics, or AI. Consumers may be surprised by the many sources of Personal Information that the Companies used to power their Algorithms, Data Analytics, or AI:

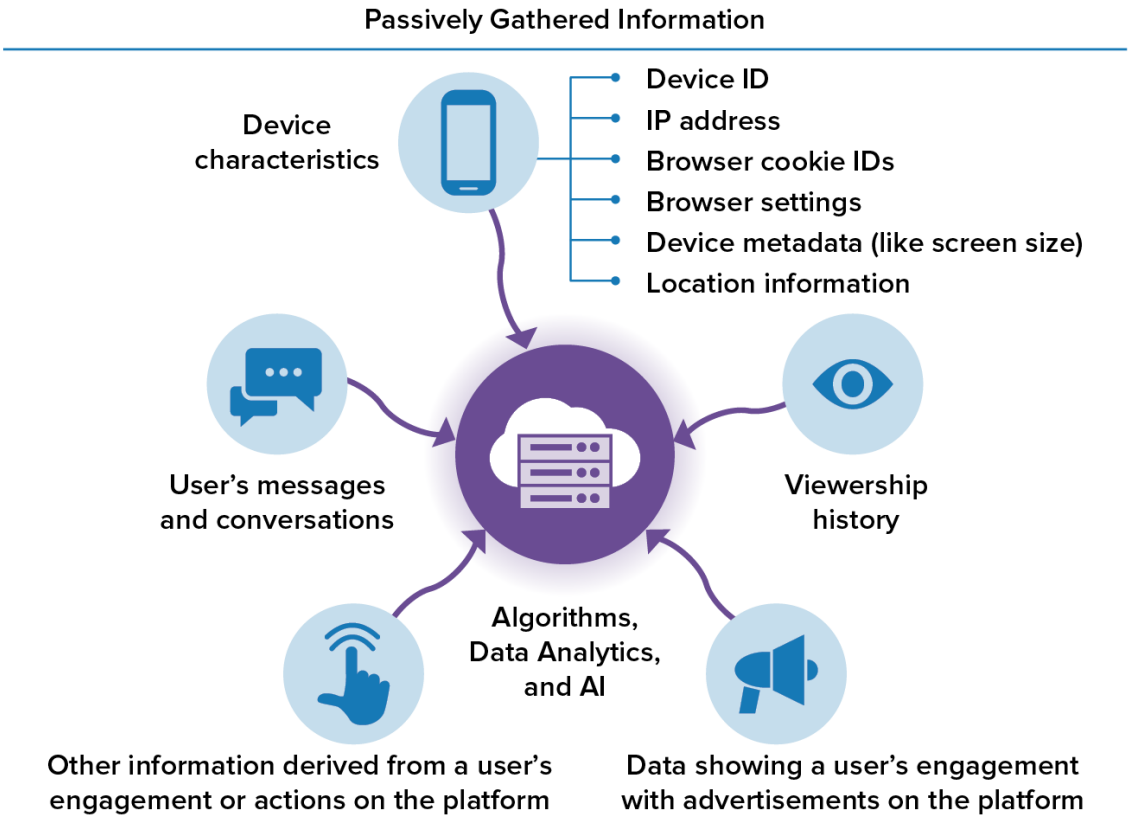
- **User-Provided Information**: Data that the user provided directly. Depending on the relevant Company, this included user-input information that the user provided to set-up an account (e.g., user inputs such as name, phone number, or date of birth) and profile information such as interests, demographic information, and profile photos.

- **Passively Gathered Information**:[233] Many Companies said their Algorithms, Data Analytics, or AI ingested information gathered passively about a user, such as information about a user's activities on the platform, which sometimes included a user's messages and conversations; device characteristics, such as device ID, IP address, browser cookie IDs, browser settings, device metadata (such as screen size) and location information; viewership

[232] *See* Section IV for more information on the Companies' data practices.

[233] Passively gathered information refers to collecting information from consumers in the background as they engage with a product, usually without their awareness. This is distinct from user-provided information, such as name, email address, or date of birth, which users typically provide directly when signing up for a service or creating an account.

history; data showing a user's engagement with advertisements on the platform; and other information derived from a user's engagement or actions on the platform.



- **User and Non-User Offline Activity**: Information about users' and non-users' activities off of the platform, such as information obtained or purchased from advertisers, data aggregators, and other third parties. Some Companies with Digital Advertising Services reported using Personal Information that third-party advertisers sent them through integrating the SMVSS's advertising tools onto their website or mobile app, which collected and sent categories of Personal Information and the user's activities and interactions with those third-party advertisers' website and mobile app properties. Once sent to the Digital Advertising Service, advertisers could use this offline data to build and customize audiences for targeted advertising on the platform, such as to build custom or lookalike audiences, and at least one SMVSS said that this data was used to train its advertising Algorithms.

- **Users' Activities on Other SMVSSs**: This included data about users and non-users from other SMVSSs, such as Personal Information they received when users connected accounts between or among other services; or when a link to content on the SMVSS was embedded on another SMVSS's app or website. At least one Company reported that the Personal Information it received from other platforms when connecting accounts was dependent on the information the user provided to the other platform and the user's account settings on that platform. At least one Company said Personal Information was transmitted only at the user's direction. The data transmitted from other SMVSSs was monetized by Companies, such as

by ingesting the information into a Company's data pipeline, and used as a data point in its Algorithms or to form data training sets.

- **Non-User Data**: Some Companies reported ingesting both user and non-user data, but at least one Company said it did not intentionally ingest non-user data. Examples included Personal Information about non-users when a user uploaded and synced their contacts list or when advertisers uploaded Personal Information (such as an email address) about all of their customers (users and non-users alike) for advertising purposes, such as to build targeted advertising audiences.

- **Inferred or Derived Data**: Some Companies also referred to creating and ingesting data that they derived or inferred about users, such as a user's preferences and interests based on their activities on the SMVSS, and other vague categories, as described in Section IV.

- **Commissioned, Purchased, or Licensed Data Sets**: In addition to data that they obtained from advertisers, Companies purchased or licensed Personal Information from third-party companies, such as data brokers and others.[234] For instance:

    - At least one Company commissioned data sets by paying third parties to collect and create data for use by its Algorithms, Data Analytics, or AI; it also reported using open-source data sets.

    - Several Companies paid third-party data brokers and others to provide data sets of Personal Information.

    - A few Companies had revenue share agreements with these third parties. For instance, these Companies integrated the third party's data into their Digital Advertising Service so that the data was available to advertisers, and paid the data providers a percentage of revenue derived from such advertising. Only one Company referenced receiving aggregated data.

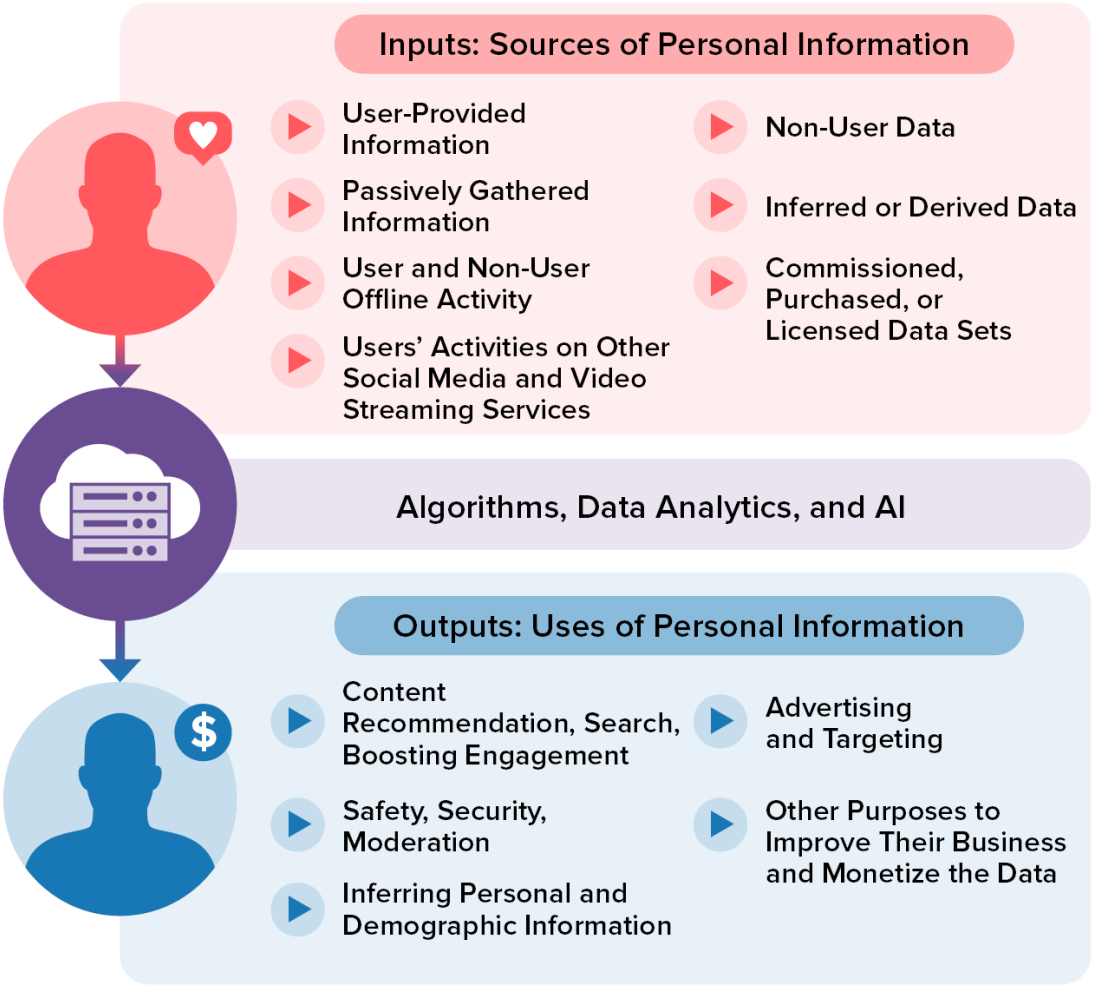
    - At least one Company represented that it obtained information such as device data and IP addresses of users and non-users to evaluate the safety and quality of content on its platform, enforce its rules, and promote security.

At least one Company claimed that the Personal Information it used for Algorithms, Data Analytics, or AI was "pseudonymized" through the application of an alias for all uses, except for safety uses, for which it used Personal Information such as IP address and unique device ID. At least one

[234] Data brokers are "companies that collect consumers' personal information and resell or share that information with others." FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Company reported that it minimized the amount of Personal Information used in its models by, whenever possible, removing information that could uniquely identify an individual.

Inputs and Outputs of Companies' Use of Algorithms, Data Analytics, or AI



C. Use of Personal Information by Algorithms, Data Analytics, or AI Raises Privacy and Other Concerns for Users and Non-Users

As a general matter, the Companies in this study collected a wide of range of Personal and Demographic Information about users and non-users, which posed risks to consumers' privacy and civil rights.[235] The broad use of this information by Algorithms, Data Analytics, or AI increases those risks. This includes, for example, potential harms and risks to consumers' civil rights, such as: the use of

[235] *See* Section IV for more information on the Companies' data practices.

skewed, unrepresentative, or imbalanced datasets that can lead to erroneous outputs; outputs that result in unlawful discrimination against certain groups;[236] opaque models that lack transparency, are "black boxes" and are not clear to the consumer (or even the developer of such tools) in terms of how they work; developers that do not understand or account for the contexts in which these tools will be used;[237] and automated decisions about individuals without their knowledge, consent, or understanding. Some of the potential privacy harms stemming from the Companies' use of information for Algorithms, Data Analytics, or AI include that automated decisions often make decisions about individuals without their knowledge, consent, or understanding and that consumers often have no recourse when it comes to biased or inaccurate data or decisions.

Trends seen among the Companies' practices that can lead to these potential harms include:

- **User and non-user information was, by default, ingested into and used by Algorithms, Data Analytics, or AI.** When it comes to using Personal Information for Algorithms, Data Analytics, or AI, the trend in the industry was that Companies did not appear to give users the choice to opt-in, nor did Companies appear to seek meaningful consent.[238] This includes user and non-user data relating to activities both on and off of the platform (including data obtained or purchased from third parties).

- **No Universal Opt-In or Opt-Out.** Another trend was that, with one exception, the Companies did not appear to offer users or non-users the opportunity to opt in or to opt out of the use of their data by Algorithms, Data Analytics, or AI.[239] In other words, the Companies

---

[236] According to the National Institute of Standards and Technology ("NIST"), which publishes an Artificial Intelligence Risk Management Framework, "fairness in AI includes concerns for equality and equity by addressing issues such as harmful bias and discrimination." NAT'L INST. OF STANDARDS & TECH., ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK 1.0, at 17 (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf. In its framework, NIST "has identified three major categories of AI bias to be considered and managed: systemic, computational and statistical, and human-cognitive. Each of these can occur in the absence of prejudice, partiality, or discriminatory intent. Systemic bias can be present in AI datasets, the organizational norms, practices, and processes across the AI lifecycle, and the broader society that uses AI systems. Computational and statistical biases can be present in AI datasets and algorithmic processes, and often stem from systematic errors due to non-representative samples. Human-cognitive biases relate to how an individual or group perceives AI system information to make a decision or fill in missing information, or how humans think about purposes and functions of an AI system. Human-cognitive biases are omnipresent in decision-making processes across the AI lifecycle and system use, including the design, implementation, operation, and maintenance of AI." *Id.* at 18. NIST's framework also acknowledges: "[w]hile bias is not always a negative phenomenon, AI systems can potentially increase the speed and scale of biases and perpetuate and amplify harms to individuals, groups, communities, organizations, and society." *Id.*

[237] *See, e.g.*, *supra* note 224, Joint Statement on Enforcement of Civil Rights, Fair Competition, Consumer Protection, and Equal Opportunity Laws in Automated Systems.

[238] While the Orders do not specifically request information about whether the Companies obtain consent, the Companies generally did not report doing so.

[239] Only one Company claimed to give its users the ability to comprehensively opt-out of use of their data via exploratory analysis, predictive analysis, and prescriptive analysis—users must have found and navigated to the service's privacy settings to opt out.

set a default policy of using consumer data for these purposes, and consumers had no real way to object.

- **Users and non-users likely did not know, did not understand, and did not control the wide-ranging collection and uses of their data by the Companies' Algorithms, Data Analytics, or AI**. This is especially true for data that these systems inferred, that was purchased from third parties, or that was derived from users' and non-users' activities off of the platform. This also holds true for non-users who did not have an account and who may have never used the relevant service.

- **Inadequate explanations of how Algorithms, Data Analytics, or AI operated**.[240, 241] As a general trend, the Companies did not, for example, appear to clearly provide to the public complete, conspicuous, and comprehensible explanations about how and why activity, inputs, and Personal and Demographic Information translated into particular automated decisions. Nor did they offer explanations of the factors that dictated a particular automated decisional outcome, both at the individual and systemic level.[242] In fact, some Companies claimed it was difficult to explain to the Commission how its models prioritized or weighed certain factors. Some Companies' unwillingness or inability to adequately explain their use of Algorithms, Data Analytics, or AI calls into question whether they can adequately explain these concepts to users and the public and whether they truly understand the technology they are implementing and its potential effects.

    - At least one Company considered the creation of an algorithmic transparency and control hub, but this was outside of the Applicable Time Period of our report. The

[240] The 2023 NIST Artificial Intelligence Risk Management Framework 1.0 refers to transparency, explainability, and interpretability as "distinct characteristics that support each other. Transparency can answer the question of 'what happened' in the system. Explainability can answer the question of 'how' a decision was made in the system. Interpretability can answer the question of 'why' a decision was made by the system and its meaning or context to the user." *Supra* note 236 at 16. *See also* Paul M. Barrett & Justin Hendrix, *Safeguarding AI: Addressing the Risks of Generative Artificial Intelligence*, NYU STERN CTR. FOR BUS. & HUM. RTS. (June 2023), https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/649c539d4af4ee01789596a9/1687966621722/NYU+CBHR+Generative+AI_June+20+ONLINE+FINAL.pdf (recommending that companies make AI system "interpretable," and stating: "[s]urprisingly, AI designers often don't understand precisely why their creations act as they do. The entire industry and the research community need to step up current efforts to solve this conundrum as part of the larger push to make models safe").

[241] In 2023, some companies announced (including a few Companies included in this study) voluntary commitments to publicly reporting their AI systems' capabilities, limitations, and areas of appropriate and inappropriate use, including security risks and societal risks, such as the effects on fairness and bias. *See* White House, FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI (July 21, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.

[242] Alex Engler, *A comprehensive and distributed approach to AI regulation*, BROOKINGS INST. (Aug. 31, 2023), https://www.brookings.edu/articles/a-comprehensive-and-distributed-approach-to-ai-regulation/.

Company noted "[o]ur industry has ignored and/or underinvested in the potential impact of algorithmic decisions on our users."

- **Potential harms from inferred sensitive data: the Companies used Algorithms, Data Analytics, or AI to profile, as well as infer or derive more personal details about individuals, such as their families, interests, income, personal relationships, and lifestyle details.** This level of profiling can lead to sensitive inferences or categorizations. This can be especially harmful to specific groups that face identity-based threats or unlawful discrimination; for instance, an Algorithm that infers an individual's sexual orientation or mental health status could cause substantial consumer harm in the form of stigma and unlawful discrimination, among others.

- **Inferring information may weaken the effectiveness of consumer choice.** If Companies are inferring information that users may have chosen not to provide in the first place, they may be subverting users' choices about their data.[243] For instance, even when consumers choose not to share information such as relationship or marital status to protect their privacy, companies may still be able to figure this out and attach such information to users without their knowledge.

- **Users and non-users did not know of and could not fix, address, or correct automated decisions about them that were inaccurate, or that may have been based on flawed or inaccurate information.** Put simply, consumers generally had no recourse when the Algorithms make inaccurate, unreliable, or biased decisions.[244] In fact, several Companies did not report any process to remove inaccurate or unauthorized data by Algorithms, Data Analytics, or AI in the advertising context. At least one Company claimed there was no risk of inaccurate or unauthorized data.

- **Security Risks**: Other systemic risks include cyber-attacks and leaks, given the concentration of extensive Personal Information collected or inferred, or the use of a Company's Algorithms, Data Analytics, or AI for nefarious purposes by hostile actors.

- **Other downstream risks**: There are further potential downstream risks, given that there are not universal legal limits on how the Companies can use Personal Information and that Companies did not have clear or specific data retention and minimization policies. Thus, new and additional uses remain possible.[245]

---

[243] *See* FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? (Jan. 2016), https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report ("Some researchers have argued that, even when companies offer consumers choices about data collection, the companies may still use big data to draw inferences about consumers who choose to restrict the collection of their data. Indeed, using data from consumers who opt in or decline to opt out, big data algorithms can still be employed to infer information about similarly-situated individuals who chose not to share their data.").

[244] Unlawful discrimination is a recognized potential harm of automated systems.

[245] *See* Section IV for more information on the Companies' data practices.

Further underscoring these potential harms, many Companies offered users no or limited transparency and control over the use of their data by Algorithms, Data Analytics, or AI. Nearly all did not report offering a comprehensive ability to directly control or opt-out of use of their data by all Algorithms, Data Analytics, or AI. Rather, some Companies' efforts were limited to allowing consumers to view or make choices relating to advertising and ad-targeting, such as opting out of targeted advertising or use of data by advertising Algorithms, or requesting to download or delete data.[246] Moreover, this required some affirmative action by the consumer, such as to find and navigate through a control or settings menu.

In addition, these opt-outs appeared limited to affecting the advertisements served to a user or preventing ad-targeting based on Personal Information on a going-forward basis, and they likely would not change decisions, inferences, or outcomes already made by an automated system, such as the detailed categories of inferred Demographic Information discussed above. Moreover, descriptions offered by some Companies were vague, with at least one indicating that consumer control affected what the consumer experienced, but it was not clear whether the Company would actually cease using their information or information that had been inferred. And at least one Company offered a limited opt-out of ad-targeting, acknowledging that it still used data inferred about individuals to advertise, even after a consumer opted out. By contrast, at least one Company did state that opting out of ad-targeting and personalization on its platform meant the removal of all historical data, activities, and interactions of the user, including inferred information, and noted that this would prevent the ad-targeting Algorithm from considering any of that information in determining ad delivery to a user and removed them from similar audience targeting. And, as noted above, even these limited opt-outs can be meaningless if they can be subverted by Algorithms, Data Analytics, or AI that can infer information that users opt out of providing.

At least one Company did reference offering consumers some explanations relating to why a consumer saw a particular ad, but this was inadequate. In particular, explanations were often vague and did not provide specificity that would allow a consumer to understand the practices at issue. Moreover, this offering failed to explain decisions made by Algorithms, Data Analytics, or AI outside of advertising.

Simply put, to the extent that Companies offered controls and opt-outs, they were insufficient to address the range of potential harms from Algorithms, Data Analytics, or AI. Among other things, such controls and opt-outs were not available outside the advertising context nor to non-users, and, for at least one SMVSS, such controls were not available at all during the Applicable Time Period of this study.

[246] *Id.*

D. Algorithms, Data Analytics, or AI that Favor Engagement Can Have Negative Mental Health Consequences for Children and Teens

As discussed above in Section VI.A.1, the Companies relied on Algorithms, Data Analytics, or AI to determine what content to serve to users. These models generally prioritized showing content that gets the most User Engagement (view time, likes, comments, or content that is trending or popular).

The Companies studied in this report that relied on targeted advertising revenue generally have an interest in serving content that drives User Engagement, because it can lead to more time on the service and greater advertising revenue.[247] Unlike contextual advertising, behavioral (i.e., targeted) advertising incentivizes continuous and constant collection of user data, which—in turn—incentivizes firms to constantly track users and to keep them engaged on the platform. For a few Companies, advertising or advertisers' goals also played some role in the presentation of user-generated content.[248]

There is evidence that certain forms of harmful content, such as dangerous online challenges, may get the most User Engagement.[249] Put another way, Algorithms that rank User Engagement over other factors can lead to the promotion and proliferation of such content, which could harm Children by keeping them online longer, among other things.

For instance, a 2023 U.S. Surgeon General Advisory Report titled "Social Media and Youth Mental Health" noted that excessive and problematic use of social media may harm Children and Teens

---

[247] Serving content that increases User Engagement can be profitable because it promotes users spending greater time on the platform, trending and viral content, greater daily or monthly active users and therefore, can draw greater advertising and advertising revenue, on which many of the Companies heavily rely.

[248] This included ensuring and prioritizing advertisers' brand safety by ensuring that only certain user-generated content can appear next to an advertiser's content. At least one Company sometimes promoted certain content (such as videos) to address commercial and product goals, such as by introducing new celebrity creators and to meet minimum commitments to advertisers, although it is not clear what this means. At least one Company permitted better placement for certain partners and affiliates.

[249] *See* Lara Kolbicke & Antonia Markiewitz, *The Momo Challenge: measuring the extent to which YouTube portrays harmful and helpful depictions of a suicide game*, 1 SN SOC. SCIS. 86 (2022), https://link.springer.com/article/10.1007/s43545-021-00065-1?utm_source=getftr&utm_medium=getftr&utm_campaign=getftr_pilot; Bonifazi et al., *Investigating Community Evolutions in TikTok Dangerous and Non-Dangerous Challenges*, J. OF INFO. SCI. (2022), https://journals.sagepub.com/doi/abs/10.1177/01655515221116519.

by disrupting important healthy behaviors[250] and lead to habit formation.[251] The report specifically noted the correlation between Algorithms and other features that prioritize User Engagement and negative health outcomes in children and adolescents:

> Social media platforms are often designed to maximize user engagement, which has the potential to encourage excessive use and behavioral dysregulation. Push notifications, autoplay, infinite scroll, quantifying and displaying popularity (i.e., 'likes'), *and algorithms that leverage user data to serve content recommendations* are some examples of these features that maximize engagement. According to one recent model, nearly a third (31%) of social media use may be attributable to self-control challenges magnified by habit formation.
>
> Further, some researchers believe that social media exposure can overstimulate the reward center in the brain and, when the stimulation becomes excessive, can trigger pathways comparable to addiction. Small studies have shown that people with frequent and problematic social media use can experience changes in brain structure similar to changes seen in individuals with substance use or gambling addictions. In a nationally representative survey of girls aged 11–15, one-third or more say they feel "addicted" to a social media platform. Over half of teenagers report that it would be hard to give up social media. Nearly 3-in-4 teenagers believe that technology companies manipulate users to spend more time on their devices. In addition, according to a survey of 8th and 10th graders, the average time spent on social media is 3.5 hours per day, 1-in-4 spend 5+ hours per day and 1-in-7 spend 7+ hours per day on social media. (emphasis added).

More research relating to these negative effects may still be forthcoming or underway. In the meantime, however, few Companies offered parents controls to guide, limit, or monitor their Teens' use of social media. In the absence of rules or laws that afford protections to Teens' privacy in the digital world, many Companies elected to treat Teens just like adults on SMVSSs.[252]

Just a few SMVSSs noted that their content recommendation and search Algorithms weighed so-called "quality" factors and signals in predicting what content to surface or promote, in addition to

---

[250] U.S. DEP'T OF HEALTH & HUM. SERVS., THE U.S. SURGEON GENERAL'S ADVISORY ON SOCIAL MEDIA AND YOUTH MENTAL HEALTH (May 23, 2023), at 9–10, https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf. *See also* Hunt Allcott et al., *Digital Addiction*, 112 AM. ECON. REV. 2424, 2424 (2022), https://pubs.aeaweb.org/doi/pdfplus/10.1257/aer.20210867 ("Temporary incentives to reduce social media use have persistent effects, suggesting social media are habit forming. Allowing people to set limits on their future screen time substantially reduces use, suggesting self-control problems. Additional evidence suggests people are inattentive to habit formation and partially unaware of self-control problems. Looking at these facts through the lens of our model suggests that self-control problems cause 31 percent of social media use.").

[251] *See* Hunt Allcott et al., *The Welfare Effects of Social Media*, 110 AM. ECON. REV. 629, 629 (2020), https://www.aeaweb.org/articles?id=10.1257/aer.20190658 ("In a randomized experiment, we find that deactivating Facebook for the four weeks before the 2018 US midterm election (i) reduced online activity, while increasing offline activities such as watching TV alone and socializing with family and friends; (ii) reduced both factual news knowledge and political polarization; (iii) increased subjective well-being; and (iv) caused a large persistent reduction in post-experiment Facebook use. Deactivation reduced post-experiment valuations of Facebook, suggesting that traditional metrics may overstate consumer surplus.").

[252] *See* Section VII for more information on the Companies' treatment of Children and Teens.

engagement-related factors. It is not clear, however, how much weight these factors received relative to engagement-related factors. Similarly unclear were the specific factors that determined whether content is "quality" in the eyes of that SMVSS, and which signals determined this trait. At least one Child-directed SMVSS similarly reported weighing quality factors in recommending content, through a machine learning quality filter and quality principles as classifiers, and it worked with outside organizations to identify high-quality content in developing these models. These models sought to prioritize and increase the discoverability of, for example, learning-related content.[253] But it was not clear how much weight these "quality" factors received in relation to User Engagement-related factors.

At least one SMVSS at one point offered users options other than an algorithmically curated news feed—it offered users the option to toggle to a news feed that served content in chronological order.[254] A few other SMVSSs only introduced similar alternatives outside the Applicable Time Period, but these options were typically not the default user experience, and users must learn how to enable and navigate to these features.[255] Other SMVSSs did not appear to offer any such alternatives. Thus, the algorithmically ranked content presentation remained the default user experience.

E. The Differing and Inconsistent Approaches to Monitoring Algorithms, Data Analytics, or AI

The Companies reported differing practices, policies, and standards for monitoring and testing their use of Algorithms, Data Analytics, or AI, such as their monitoring and testing for bias, reliability, and accuracy. Overall, there was no uniform or standard approach. And, in general, the Companies'

[253] At least one Company described another approach: using a machine learning model to downrank what it considered to be unhealthy conversations on its platform.

[254] Casey Newton, *Twitter is relaunching the reverse-chronological feed as an option for all users starting today*, THE VERGE (Dec. 18, 2018), https://www.theverge.com/2018/12/18/18145089/twitter-latest-tweets-toggle-ranked-feed-timeline-algorithm.

[255] Sarah Perez, *Instagram launches chronological and 'favorites' feeds for all users, but they can't be the default,* TECHCRUNCH (Mar. 23, 2022), https://techcrunch.com/2022/03/23/instagram-launches-chronological-and-favorites-feeds-for-all-users-but-they-cant-be-the-default/.

inconsistent approaches to monitoring and testing stood in contrast to recent calls for transparency and testing standards.[256]

1. The Responsible People and Oversight Structures Varied—Only Some Had Dedicated AI-Specific Teams

While some Companies reported dedicating robust resources to the oversight of Algorithms, Data Analytics, or AI, others did not.

Some Companies reported internal teams or organizations dedicated to company-wide oversight of Algorithms, Data Analytics, or AI, such as to address concerns relating to ethics, bias, inclusion, and fairness in the use of these technologies in their products. For instance, this included large teams of in-house experts, such as ethicists, social and political scientists, policy experts, AI researchers, and engineers. Some Companies reported that specific teams were responsible for the development, review, or oversight for specific Algorithms, Data Analytics, AI, or machine learning models.

By contrast, some Companies did not have dedicated internal AI- or machine learning-specific teams or organizations. Among these, some reported that responsibility for oversight rested across several teams such as the engineering, privacy, product, legal, policy, and governance teams. Some Companies reported a lack of infrastructure or oversight surrounding their use of Algorithms, Data Analytics, or AI. At least one of these Companies reported that it did not focus on algorithmic bias (saying that it was not heavily reliant on Algorithms or content ranking). At least one Company described attempting to educate teams that used machine learning, and described internal oversight efforts that seem aspirational. And at least one did not report any testing, ethics, or compliance programs regarding Algorithms, Data Analytics, or AI.

But even where Companies reported dedicating robust internal resources to Algorithms, Data Analytics, or AI, the authority of these internal organizations was not always clear, and their role appeared limited to consulting and offering guidance to the teams that developed the models. It also was not clear whether any of their recommendations were binding.

2. The Frequency of Testing Varied Widely

When it came to monitoring, testing, or validating the accuracy or effects of their Algorithms, Data Analytics, or AI, most Companies described doing so regularly or on an ongoing basis. Some also described regularly or constantly updating and modifying these automated tools. Although Companies described this testing as regular, constant, or ongoing, the frequency sometimes varied, and differed based on the algorithmic model at issue. Thus, there was not a clear or common meaning of what regular, constant, or ongoing testing meant. A few Companies validated reliability and accuracy of their Algorithms, Data Analytics, or AI on an ad-hoc basis or stated that their monitoring and testing occurred

[256] White House, FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosam&stream=top.

when warranted and with no set frequency; at least one other stated that it regularly reviewed and updated Algorithms, Data Analytics, or AI that were core to its business (without specifying what it considers "core to its business").

3. The Way Companies Monitored and Tested Also Varied

The Companies also noted various ways by which they identified and addressed privacy, security, or bias, ethics, accuracy, or reliability issues posed by applying Algorithms, Data Analytics, or AI to Personal Information. The most common means of identifying and addressing issues were through use of automated tools; A/B testing; human review; training and educating teams using Algorithms, Data Analytics, or AI; and engaging in privacy reviews.

Methods for how the Companies reviewed, measured, and assessed bias concerns, such as how the use of Algorithms, Data Analytics, or AI can express bias or effects relating to race, age, gender, and other categories, also differed. Some Companies reported using automated testing tools. A few Companies reported use of specific automated software tools or programs that were designed to help the Company measure and test for bias in their products. Some Companies reported focusing their bias testing efforts on age, gender, or race. For instance, some Companies reported testing Algorithms to make cameras that work better for users with darker skin tones or noted they were in the process of learning how to improve machine vision systems that work well for a variety of skin tones.

On the other hand, some Companies did not report having any established process to monitor or test for bias. At least one Company reported that it did not test for bias during the Applicable Time Period. Other Companies' descriptions of efforts at identifying and combatting bias were vague or not specific; at least one Company developed a program to tackle bias and underrepresentation, but this was outside the Applicable Time Period. Finally, at least one Company has said it did not identify any bias through its testing.

Moreover, the Companies largely did not report conducting comprehensive audits of their use of Algorithms, Data Analytics, or AI, or of their monitoring and testing capabilities. Most Companies did not report hiring independent third parties to review or audit their capabilities or conducting adversarial testing.[257] At least one Company referenced establishing a "bounty program" as a way to identify harm, such as an algorithmic bias bounty challenge, which incentivized members of the public to identify potential harms in its use of Algorithms, Data Analytics, or AI.[258]

---

[257] As noted in a May 2023 White House Fact sheet on AI initiatives, testing of AI models independent of government or the companies that have developed them is an important component in their effective evaluation. White House, FACT SHEET: Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation that Protects Americans' Rights and Safety (May 4, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety/. In 2023, some companies announced (including a few included in this study) voluntary commitments relating to their monitoring and use of AI, such as committing to internal and external security testing of their AI systems before their release. *Supra* note 241.

[258] This bounty program was introduced after the Applicable Time Period of this report.

While the Companies acknowledged that their Algorithms, Data Analytics, or AI processed actual or inferred Personal and Demographic Information, many offered vague descriptions of their testing, training, and retraining of models for bias and accuracy or vague descriptions of how they ensure their models were trained by data sets that were representative and not missing information. At least one Company stated that it did not examine whether data sets were missing information from particular populations, and at least one Company noted that it relied on publicly available datasets to train certain of its Algorithms. Some offered non-specific descriptions, stating, for example, that they sought to utilize balanced training data sets to reduce the likelihood of missing information from particular or underrepresented populations; that they sought to validate certain findings with underrepresented communities and revise Algorithms accordingly; that they worked to address whether data sets were missing data from particular groups or underrepresented populations, and that doing so was challenging without processing sensitive user data; or that they did not rely on fixed data for training, but instead used a system that picked from millions of current pieces of content.

By the same token, some Companies also offered vague descriptions of how they remedied problems they detected or that were brought to their attention, such as stating that they took steps to mitigate the result of detected bias, without further explanation, or offered no explanation of how they trained or retrained flawed models. This vagueness is contrary to calls for companies to be transparent about training data and methods.[259]

4. Companies Reported Limited Human Review

Most Companies referred to some level of human review or involvement in monitoring, testing, and reviewing decisions made by Algorithms, Data Analytics, and AI. But some Companies provided more specifics than others (with some offering vague descriptions of the role of human reviewers), and the scope, level of involvement, and overall effects of human reviewers on automated processes differed.

Most Companies used human review in limited contexts. Human review was most often reported in the context of Algorithms, Data Analytics, and AI relating to content moderation, such as sampling the outputs of the system's decisions. But it was not always clear how and at what stage human reviewers came into the picture; whether only certain decisions already made by automated systems were subject to human review; and which automated decisions were not subject to human review. A few also reported relying in part on automated systems to flag content for human review. Outside of content moderation, only a few Companies mentioned using human review for other functions, such as to monitor, test, assess, and manually change decisions made by content recommendation and search Algorithms or for purposes of reviewing ad placement to protect brand safety.

---

[259] *See* Paul M. Barrett & Justin Hendrix, *Safeguarding AI: Addressing the Risks of Generative Artificial Intelligence*, NYU STERN CTR. FOR BUS. & HUM. RTS. (June 2023), https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/649c539d4af4ee01789596a9/1687966621722/NYU+CBHR+Generative+AI_June+20+ONLINE+FINAL.pdf.

Moreover, it was often unclear whether the majority of decisions made by Algorithms, Data Analytics, or AI were subject to some form of human review. Even assuming human review was involved, the Companies did not specify the qualifications of reviewers, whether reviewers were employees or external to the Company, and whether reviewers represented diverse backgrounds, viewpoints, and perspectives. Given the limited and vague information the Companies submitted, it was not clear whether human reviewers were empowered to meaningfully change or alter flawed models. NIST, which has published an Artificial Intelligence Risk Management Framework, has noted the risks of AI actors bringing their own biases to the table, and the potential for AI to magnify those effects: "[b]iases can stem from end-user decision-making tasks and be introduced across the AI lifecycle via human assumptions, expectations, and decisions during design and modeling tasks. These biases, which are not necessarily always harmful, may be exacerbated by AI system opacity and the resulting lack of transparency."[260]

F. Key Findings

This section makes the following key findings, although each finding may not be applicable to every one of the Companies in every instance.

- **Many Companies have relied heavily on the use of Algorithms, Data Analytics, or AI—and the ingestion of Personal Information—to power their SMVSSs.** In short, automated systems have dictated much of the user's experiences, even if the user experience on each SMVSS may be different. Automated systems have determined what user-generated content and advertisements to display and remove. These systems also inferred or predicted personal details about users and their lives, such as their interests, habits, demographic categories, familial status and relationships, employment and income details, and likely other details and information not provided by the Companies.

- **The Companies generally fed extensive amounts of Personal Information into their automated systems, some of which was sourced from the users themselves—but they also often collected information passively about users' and non-users' activities across the Internet and in the real world (i.e., location information), and some Companies collected information from data brokers and other third parties.** Companies implemented a default policy of using consumers' Personal Information, without giving consumers the opportunity to opt in or to opt out. They also created new and potentially sensitive data points about individuals by inferring information. Moreover, the seeming inability or failure of Companies to adequately and easily explain their use of Algorithms, Data Analytics, or AI raises its own set of questions about their own responsible and safe use of these technologies.

- **Consumer harms are further compounded where systems have the effect of being biased or unreliable, or where they can be used to infer sensitive information about individuals, such as by labeling them into sensitive demographic categories**. This can

[260] *See supra* note 236.

lead to threats, stigma, embarrassment, unwanted tracking or profiling, unlawful discrimination, and other potential harms, which can be especially harmful to specific groups that face identity-based threats.

VII. Children and Teens

While many SMVSSs state that they are only for those thirteen and over, it is well known that both Children[261] and Teens[262] use them, including those SMVSSs that are part of this study. Research indicates that approximately 95% of teenagers and 40% of children between the ages of eight and 12 years old use some form of social media.[263] While the use of social media and digital technology can provide many positive opportunities for self-directed learning, forming community, and reducing isolation, it also has been associated with harms to physical and mental health, including through exposure to bullying, online harassment, child sexual exploitation, and exposure to content that may exacerbate mental health issues, such as the promotion of eating disorders, among other things.[264] Another survey of American Teens reported that more than half say that it would be difficult for them

---

[261] *See supra* note 118 (definition of Child or Children). *See, e.g.*, Amanda Raffoul et al., *Social media platforms generate billions of dollars in revenue from U.S. youth: Findings from a simulated revenue model*, PLoS ONE (Dec. 27, 2023), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0295337; U.S. DEP'T OF HEALTH & HUM. SERVS., THE U.S. SURGEON GENERAL'S ADVISORY ON SOCIAL MEDIA AND YOUTH MENTAL HEALTH (May 23, 2023), https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf; Colleen McClain, *How parents' views of their kids' screen time, social media use changed during COVID-19*, PEW RES. CTR. (Apr. 28, 2022), https://www.pewresearch.org/short-reads/2022/04/28/how-parents-views-of-their-kids-screen-time-social-media-use-changed-during-covid-19/; *The Common Sense Census: Media Use by Tweens and Teens* 22, COMMON SENSE MEDIA (2021), https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf.

[262] *See supra* note 123 (definition of Teen). *See, e.g.*, Jonathan Rothwell, *Teens Spend Average of 4.8 Hours on Social Media Per Day,* GALLUP (Oct. 13, 2023), https://news.gallup.com/poll/512576/teens-spend-average-hours-social-media-per-day.aspx; U.S. DEP'T OF HEALTH & HUM. SERVS., THE U.S. SURGEON GENERAL'S ADVISORY ON SOCIAL MEDIA AND YOUTH MENTAL HEALTH (May 23, 2023), https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf; Emily A. Vogels & Risa Gelles-Watnick, *Teens and social media: Key findings from Pew Research Center surveys*, PEW RES. CTR. (Apr. 24, 2023), https://www.pewresearch.org/short-reads/2023/04/24/teens-and-social-media-key-findings-from-pew-research-center-surveys/; Monica Anderson et al., *Teens, Social Media and Technology 2023*, PEW RES. CTR. (Dec. 11, 2023), https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/.

[263] U.S. DEP'T OF HEALTH & HUM. SERVS., THE U.S. SURGEON GENERAL'S ADVISORY ON SOCIAL MEDIA AND YOUTH MENTAL HEALTH (May 23, 2023), https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf. *See also* Amanda Raffoul et al., *Social media platforms generate billions of dollars in revenue from U.S. youth: Findings from a simulated revenue model*, PLoS ONE (Dec. 27, 2023), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0295337.

[264] U.S. DEP'T OF HEALTH & HUM. SERVS., THE U.S. SURGEON GENERAL'S ADVISORY ON SOCIAL MEDIA AND YOUTH MENTAL HEALTH (May 23, 2023), https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf; Emily A. Vogels, *Teens and Cyberbullying 2022*, PEW RES. CTR (Dec. 15, 2022), https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/; Jacqueline Nesi et al., *Social Media Use and Self-Injurious Thoughts and Behaviors: A Systematic Review and Meta-Analysis*, 87 CLINICAL PSYCHOL. REV. 102038 (2021), https://www.sciencedirect.com/science/article/abs/pii/S0272735821000817?via%3Dihub.

to give up social media.[265] And this works in social media services' favor as Teens are an increasingly valuable demographic for advertisers because of their spending power.[266]

As Child and Teen use of social media increases, so do the concerns regarding such use and the potential harms to Children and Teens.[267] There is the concern that adults will use social media to exploit Children or Teens.[268] Another serious concern is the potential effect of social media use on mental health; in fact, a 2019 study found that adolescents spending more than three hours per day on social media was associated with increased mental health problems.[269] It comes as no surprise that

---

[265] Emily A. Vogels & Risa Gelles-Watnick, *Teens and social media: Key findings from Pew Research Center surveys*, PEW RES. CTR (Apr. 24, 2023), https://www.pewresearch.org/short-reads/2023/04/24/teens-and-social-media-key-findings-from-pew-research-center-surveys/.

[266] *See, e.g.*, Jeff Fromm, *As Gen Z's Buying Power Grows, Businesses Must Adapt Their Marketing*, FORBES (July 20, 2022), https://www.forbes.com/sites/jefffromm/2022/07/20/as-gen-zs-buying-power-grows-businesses-must-adapt-their-marketing/?sh=3eb5394d2533; Amelia Pollard, *Gen Z Has $360 Billion to Spend, Trick is Getting Them to Buy*, BLOOMBERG (Nov. 17, 2021), https://www.bloomberg.com/news/articles/2021-11-17/gen-z-has-360-billion-to-spend-trick-is-getting-them-to-buy.

[267] *See* Colleen McClain et al., *How Americans View Data Privacy*, PEW RES. CTR. (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/ (finding that 89% of U.S. adults surveyed are very or somewhat concerned about social media platforms knowing personal information about kids). *See generally* Elena Bozzola et al., *The Use of Social Media in Children and Adolescents: Scoping Review on the Potential Risks*, 19 INT'L J. OF ENVTL. RES. & PUB. HEALTH 9960 (2022), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9407706/pdf/ijerph-19-09960.pdf.

[268] *See, e.g.*, Press Release, U.S. Att'y's Off. S.D. Ohio, U.S. Attorney warns about rise in online impersonators exploiting children (June 27, 2023), https://www.justice.gov/usao-sdoh/pr/us-attorney-warns-about-rise-online-impersonators-exploiting-children; Press Release, Fed. Bureau of Investigation, International Law Enforcement Agencies Issue Joint Warning about Global Financial Sextortion Crisis (Feb. 7, 2023), https://www.fbi.gov/news/press-releases/international-law-enforcement-agencies-issue-joint-warning-about-global-financial-sextortion-crisis.

[269] Kira E. Riehm et al., *Associations Between Time Spent Using Social Media and Internalizing and Externalizing Problems Among US Youth*, 76 JAMA PSYCHIATRY 1266 (2019), https://jamanetwork.com/journals/jamapsychiatry/fullarticle/2749480. *See also* U.S. DEP'T OF HEALTH & HUM. SERVS., THE U.S. SURGEON GENERAL'S ADVISORY ON SOCIAL MEDIA AND YOUTH MENTAL HEALTH (May 23, 2023), https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf; *Health Advisory on Social Media Use in Adolescence*, AM. PSYCHOL. ASS'N (May 2023), https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use.pdf; Monica Anderson et al., *Connection, Creativity and Drama: Teen Life on Social Media in 2022*, PEW RES. CTR. (Nov. 16, 2022), https://www.pewresearch.org/internet/2022/11/16/connection-creativity-and-drama-teen-life-on-social-media-in-2022/.

Other potential harms include distracting students from school. One study of 11- to 17-year-olds found that 32% of smartphone use during school hours was for social media platforms. Another 26% of smartphone use during school hours was for students using YouTube. Another potential harm is that such students use their smartphones overnight (between the hours of midnight and five a.m.) on school nights, primarily to access social media (39%) and YouTube (47%). Another potential harm is tween (11-to-13-year-olds) exposure to inappropriate experiences (e.g., apps rated for Teens or higher), including TikTok, Snapchat, Discord, Instagram, Facebook, and Reddit. Common Sense Media, *Constant Companion: A Week in the Life of a Young Person's Smartphone Use*, COMMON SENSE MEDIA (2023), http://www.commonsensemedia.org/sites/default/files/research/report/2023-cs-smartphone-research-report_final-for-web.pdf.

surveys have found that 81% of U.S. adults and 46% of U.S. Teens support social media companies requiring parental consent for minors to create a social media account.[270]

This section reviews the Companies' responses regarding their policies and practices with respect to Children and Teens.[271] First, we review the Companies' reported intended SMVSS audiences and user bases[272] and compare that to any information in the Companies' possession regarding the actual age of their user bases.[273] Second, we examine the Companies' reported policies and procedures with respect to Child or Teen users.[274] Third, we review the Companies' reported policies and procedures with respect to the parents or legal guardians of Child/Teen users.[275] Fourth, we discuss the Companies' reported membership in any self-regulatory organizations or programs related to Children's privacy.[276] We conclude by offering some key findings regarding the Companies' practices with respect to Child and Teen SMVSS users.

Most of the SMVSSs at issue in this report stated that they were not intended for Children[277] and that their intended user age was thirteen or older.[278] A few Companies reported their SMVSSs as being "general audience"[279] services. No Company reported that the intended user age for its SMVSS, or those allowed to create accounts, had to be over the age of eighteen. Only a few SMVSSs reported that their intended user age was less than thirteen years old, or that their service was otherwise directed to Children. Overall, most Companies reported that their SMVSSs were not directed to Children or to Teens, but they nevertheless permitted anyone thirteen or over to create an account with few limitations, as discussed below.

---

[270] Monica Anderson & Michelle Faverio, *81% of U.S. adults – versus 46% of teens – favor parental consent for minors to use social media*, PEW RES. CTR. (Oct. 31, 2023), https://www.pewresearch.org/short-reads/2023/10/31/81-of-us-adults-versus-46-of-teens-favor-parental-consent-for-minors-to-use-social-media/. These surveys also found that 71% of U.S. adults and 56% of U.S. Teens surveyed support requiring people to verify their age before using social media sites.

[271] The current study did not examine the effects of SMVSS use on Children or Teens.

[272] *See* Appendix A, Specification Nos. 44(a), 45(a), 48.

[273] *See* Appendix A, Specification No. 45(b).

[274] *See* Appendix A, Specification No. 44(b).

[275] *See* Appendix A, Specification No. 46.

[276] *See* Appendix A, Specification No. 47.

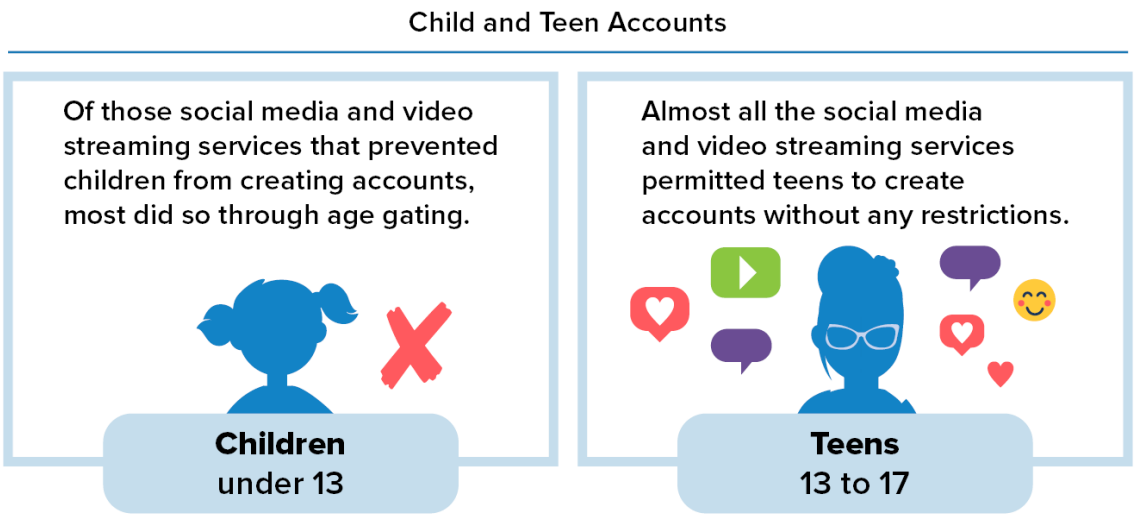
[277] Operators of web sites or online services directed to Children, or with actual knowledge that they are collecting or maintaining personal information from a Child, are required to comply with the COPPA Rule. *See* 16 C.F.R. pt. 312.

[278] Although most SMVSSs reported that users aged thirteen or older could create accounts, many SMVSSs also stated that their services were not directed to Teens.

[279] A "general audience" website or service is a website or service that, for purposes of the COPPA Rule, is not directed to children. *See* 16 C.F.R. § 312.2 (defining "web site or online service directed to children").

The Order also sought to investigate what age information the Companies, and their SMVSSs, possessed regarding their users.[280] Only one Company reported not possessing any age information at all regarding its SMVSS users, meaning that most SMVSSs had some information regarding their users' ages. Most Companies reported that they collected date of birth information from users, either as required through age gating or as part of the registration process or optional as part of profile creation. Several Companies reported inferring users' age range (e.g., thirteen to seventeen years old) either by using Algorithms, Data Analytics, or AI,[281] or from third-party analyses. Of the Company SMVSSs that inferred age using Algorithms, Data Analytics, or AI, or from third-party analyses, some reported inferring an age range less than thirteen years old. The remaining Company SMVSSs inferred only age ranges above thirteen years old. This choice by Companies demonstrates willful blindness around Child users as there is no technological impediment to inferring ages less than thirteen years old. It is possible that such SMVSSs refused to infer any age range below thirteen years old for the fear of being deemed to have "actual knowledge" under the COPPA Rule and thus being liable for such legal requirements.[282] This leads to the absurd result wherein the Companies stated that their Algorithms, Data Analytics, or AI could detect if a user was between 13 and 14 years of age, but if a user was under thirteen then the Companies stated they had to rely on other means (e.g., self-reporting) to determine that a user was a Child.

A. Policies and Procedures for Child and Teen Users



[280] *See* Appendix A, Specification No. 45.

[281] *See* Section VI for more information on the Companies' practices with respect to Algorithms, Data Analytics, or AI.

[282] *See, e.g.*, 16 C.F.R. § 312.3 ("It shall be unlawful for any operator of a Web site or online service directed to children, *or any operator that has actual knowledge that it is collecting or maintaining personal information from a child*, to collect personal information from a child in a manner that violates the regulations prescribed under this part." (emphasis added)).

1. The Companies Generally Restricted Children from Creating SMVSS Accounts and Afforded Them Other Protections

Most Companies reported preventing, or blocking, Children from creating accounts on their SMVSSs. Of those SMVSSs that prevented Children from creating accounts, most did so through age gating. Age gating refers to a process wherein a service requires a user to enter or provide their age or date of birth when they attempt to register for a service. For the SMVSSs that age gated, if a user entered an age or date of birth younger than thirteen, then the SMVSS would block the user from creating an account with the SMVSS. Some of these SMVSSs went further and implemented practices to prevent Children from circumventing the age gate, primarily by placing a cookie on the browser to restrict repeat registration attempts. A few Companies reported that they only contractually prohibited Children from creating accounts on an SMVSS, meaning that there was no actual mechanism in place to stop a Child from creating an account.[283]

Only a few Companies reported that Children could have accounts on their SMVSS. Such Companies allowed the creation of Child accounts either by the parent by obtaining verifiable consent[284] or by placing such Children in a separate user experience designed for Children. Only one Company reported that their SMVSS had ever relied on verifiable parental consent provided by an educational institution.[285]

The primary policy or practice implemented by the SMVSSs with respect to users who indicated they were under the age of thirteen was to prevent or prohibit said user from creating an account. If a Child managed to create an account, most of these SMVSSs provided other users with a means to report the underage user. A few SMVSSs reported using other methods to discover Child users, including having the SMVSS content reviewers flag content that appeared to come from an underage user or tracking when a user changed their date of birth to be under thirteen years old. Regardless of how these SMVSSs came to know that a Child user was behind an account, another common policy or practice reported by such SMVSSs was that they would disable or lock these accounts as soon as they became aware that a user was potentially a Child.[286] Some of these SMVSSs reported that they gave the user the opportunity to prove that they were, in fact, not a Child. Most, but not all, of these SMVSSs reported

---

[283] Such SMVSSs stated that their privacy policies or terms of service stated that Children are not to use their services, but they did not implement any form of age gating or other mechanism to prevent Children from registering for accounts.

[284] The COPPA Rule defines "Obtaining Verifiable Consent" as "making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child: (1) Receives notice of the operator's personal information collection, use, and disclosure practices; and (2) Authorizes any collection, use, and/or disclosure of the personal information." 16 C.F.R. § 312.2.

[285] Educational institutions may "act as the parent's agent and can consent under COPPA to the collection of kids' information on the parent's behalf" where "an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose." *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

[286] A smaller subset of SMVSSs reported that the SMVSS itself would investigate whether the user appeared to be a Child prior to suspension.

that they ultimately deleted the account. A few SMVSSs reported that they would also ban the user or direct the user to the SMVSS's Child-directed platform.

As expected, the policies and practices implemented by SMVSSs that permitted users under thirteen to create accounts, versus those that do not, were quite different. Most of the SMVSSs that allowed Children to have accounts either prohibited advertising with respect to their Child users or prohibited targeted advertising. Their other reported policies and practices included limiting data collection and ensuring that the SMVSS username could not act as a means of contacting the Child, practices that closely align with the COPPA Rule.

2. The Companies Generally Did Not Restrict Teens from Creating SMVSS Accounts and Treated Them Like Adult Users

Almost all the SMVSSs permitted Teens to create accounts without any restrictions. Only a very small number of Child-directed Company SMVSSs either did not allow Teens to have accounts or required an adult over the age of 18 to create an account for the Teen. All "general audience" Company SMVSSs allowed Teens to create accounts and did not require any affirmative parental consent or explicit involvement.[287]

Only one Company reported that it would respond should it come to find out that a Teen user had created an account without parental consent. This Company would suspend the account and ultimately delete the account and any personal information unless the user was able to appeal the suspension successfully. Most Companies explicitly reported that they would not do anything if they learned that a Teen user had created an SMVSS account without parental consent.

Of the Companies that allowed Teens to create accounts on their SMVSSs, they all collected Personal Information from Teens in the same manner as they collected Personal Information from adult users. When asked about their data collection practices with respect to Teen users, many Companies cited or referenced their SMVSS's general privacy policies. This indicates that these Companies did not consider Teens to be distinct or different from adult users with respect to data collection and use practices and processed Teen user data as if it were adult user data, despite the potential effects on Teen mental health,[288] and the fact that, more than half said it would be difficult for them to give up social media even though surveys indicate that many Teens feel that they have little or no control over the personal information that social media companies collect about them.[289]

---

[287] One Company reported that its SMVSS terms of service required that Teen users agree that their legal guardian had reviewed and agreed to the SMVSS's terms of service.

[288] *See supra* note 269.

[289] Emily A. Vogels & Risa Gelles-Watnick, *Teens and social media: Key findings from Pew Research Center surveys*, PEW RES. CTR. (Apr. 24, 2023), https://www.pewresearch.org/short-reads/2023/04/24/teens-and-social-media-key-findings-from-pew-research-center-surveys/. *See also*, Monica Anderson et al, *Connection, Creativity and Drama: Teen Life on Social Media in 2022*, PEW RES. CTR. (Nov. 16, 2022), https://www.pewresearch.org/internet/2022/11/16/connection-creativity-and-drama-teen-life-on-social-media-in-2022/.

Beyond data collection practices, about half of the Companies' SMVSSs implemented additional protective measures specific to Teen users.[290] The most common additional protective measure for Teens was preventing or limiting access to adult content or adult features. Another, although less common, additional protective measure for Teens was imposing stricter privacy settings by default (e.g., establishing an SMVSS account to private by default). Some Companies reported different advertising practices with respect to Teen users of their SMVSS, such as limiting the types of ads that could be seen by the Teen user. A few Companies had additional protective measures for Teen users that were specific to how the Teen user could share content through the SMVSS or the means by which the Teen user could communicate with other SMVSS users.

B. Policies and Procedures for Parents or Legal Guardians of Child/Teen Users

1. Most Companies Gave Some Rights to Parents/Legal Guardians With Respect to Child Users

Only some Company SMVSSs had a process by which a parent or legal guardian could request to access or review the Personal Information collected from their Child. For those few SMVSSs that did provide this process, there was no consistent means by which a parent or legal guardian could submit this request.[291] All Child-directed SMVSSs provided parents or legal guardians with the ability to access or review the Personal Information collected from their Child.[292]

Most Company SMVSSs had a process by which a parent or legal guardian could request the deletion of Personal Information collected from their Child.[293] Of the SMVSSs that had such a process, most either required the parent or legal guardian to make said request by email or through an established web form. Some Company SMVSSs reported that in order to fulfill the parent or legal guardian's request to delete the Personal Information collected from the Child, the parent or legal guardian would have needed to provide the Child's username on the SMVSS. Other Company SMVSSs required that the parent or legal guardian provide verification (e.g., Child's date of birth), and a few even required the parent or legal guardian to prove ownership of the phone number connected to the SMVSS.

---

[290] Some SMVSSs reported protective measures that are applicable to all users, not specifically for Teens. We did not include such measures in our discussion as they were not developed specifically with the intention of providing a safer experience for Teen users on the SMVSS.

[291] For example, SMVSSs would receive such parent or legal guardian requests via email, established web form, or by directing the parent or legal guardian to make the request directly in the SMVSS mobile application.

[292] The COPPA Rule requires that all Child-directed web sites or online services "[p]rovide a reasonable means for a parent to review the personal information collected from a child . . . ." 16 C.F.R. §312.3(c). *See also* 16 C.F.R. § 312.6.

[293] The COPPA Rule also requires that all Child-directed web sites or online services provide a parent "[t]he opportunity at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information . . . ." 16 C.F.R. § 312.6(a)(2).

2. Very Few Companies Gave Any Rights to Parents/Legal Guardians of Teen Users

Some Company SMVSSs would allow parents or legal guardians to review or access the Personal Information collected from a user under the age of eighteen, but would require that the parent or legal guardian verify both the parent/legal guardian's and Teen user's identities.

Even less common was a Company allowing a parent or legal guardian to request that the SMVSS delete the Personal Information collected from a Teen user. Most Companies reported that they either would not fulfill a parent or legal guardian's request to delete a Teen user's data or required all such requests to come through the Teen user's account (and thus presumably through the Teen).

C. Self-Regulatory Organizations

Most Companies reported that they were not members of any self-regulatory organizations or programs related to Children's privacy. Of the very few Companies that reported being members of any Children's privacy organizations or programs, most of those programs had to do either with child sexual abuse material or exploitation or helping keep Children safe online.

D. Key Findings

This section makes the following key findings, although each finding may not be applicable to every one of the Companies in every instance.

- **SMVSSs bury their heads in the sand when it comes to Children using their services.** Most SMVSSs suggested that, because they were not directed to children and did not allow Children to create accounts, there were no Child users. This is not credible. It is well known that Children are using SMVSSs.

- **Only some SMVSSs had a process by which parents/legal guardians could request access to the Personal Information collected from their Child.** While most of the Company SMVSSs had a process for parents/legal guardians to request the deletion of Personal Information collected from their Child, such processes varied across SMVSSs, likely making it so that parents/legal guardians were left to figure things out on their own.

- **The SMVSSs often treated Teens as if they were traditional adult users.** Children do not become fully formed adults the moment they turn thirteen, and the harms Congress enacted COPPA to prevent[294] can affect teenagers as much as—or even more than—they affect Children. Research indicates that teens' digital lives may result in safety, mental health, and privacy

[294] Among other things, COPPA was enacted to protect the privacy of children in the online environment, to protect the safety of children online, and to maintain the security of personally identifiable information of children collected online. *See* 144 CONG. REC. S12,787 (daily ed. Oct. 21, 1998) (statement of Sen. Bryan), https://www.congress.gov/105/crec/1998/10/21/144/151/CREC-1998-10-21-senate.pdf.

harms.[295] This is especially notable given that young people, including Teens, are reporting higher prevalence of mental health conditions than adults.[296]

VIII. Competition Implications

How companies approach the foregoing issues, including their data collection, data use, and privacy practices, can also be relevant to competition analysis. As discussed throughout this report, not all such practices are created equal—some are better for consumers than others. Further, these practices can be an important part of the overall quality of a company's product offering, and as with other dimensions of price and quality, competition can spur companies to provide more consumer-friendly terms and protections. These dynamics can exist, moreover, regardless of whether companies offer their products to consumers using a "zero price" model, a "freemium" model, or by charging all consumers a monetary price for the product.

Lack of competition, in turn, can lead to consumer harm. When companies eliminate competitive threats and do not face adequate competitive checks, quality, innovation, and customer service suffer. Competition is harmed by unlawful mergers or illegal agreements that lead to market power and decreased competition. Competition is also impaired when dominant firms exclude actual or potential rivals through exclusionary or other unlawful conduct. For instance, an acquisition or conduct that impairs a rival or potential rival may limit competition that would otherwise spur companies to improve and distinguish themselves along these dimensions in ways that benefit consumers—e.g., by collecting less data or providing consumers with greater control over how their data is used. In sum, limited competition can exacerbate the consumer harm described throughout this report.

Further, in digital markets, including AI, acquiring and maintaining access to significant user data can be a path to achieving market dominance and building competitive moats that lock out rivals.[297]

---

[295] *See, e.g.*, Press Release, Fed. Bureau of Investigation, FBI Charlotte Warns Sextortion Attempts Likely to Increase During Holiday Break (Dec. 27, 2023), https://www.fbi.gov/contact-us/field-offices/charlotte/news/fbi-charlotte-warns-sextortion-attempts-likely-to-increase-during-holiday-break (warning that financial sextortion cases targeting teenage boys were increasing); Emily A. Vogels, *Teens and Cyberbullying 2022*, PEW RES. CTR. (Dec. 15, 2022), https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/ (finding that 46% of U.S. teens have experienced cyberbullying); Eleva Savoia et al., *Adolescents' Exposure to Online Risks: Gender Disparities and Vulnerabilities Related to Online Behaviors*, 18 INT. J. ENVIRON. RESEARCH & PUBLIC HEALTH 5786 (2021), https://www.mdpi.com/1660-4601/18/11/5786 (finding that 62% of participants, in 8th and 9th grade, had chatted with strangers on social media, and that 31% had "shared personal information, such as their school or town name when posting on social media").

[296] *See, e.g.*, *Mental health and young people*, ORGANISATION FOR ECON. CO-OPERATION & DEV., https://www.oecd.org/coronavirus/en/data-insights/mental-health-and-young-people; Jonathan Rothwell, *How Parenting and Self-Control Mediate the Link Between Social Media Use and Youth Mental Health*, INST. FOR FAMILY STUDIES (Oct. 11, 2023), https://ifstudies.org/ifs-admin/resources/briefs/ifs-gallup-parentingsocialmediascreentime-october2023-1.pdf (stating that "[t]he mental health of U.S. teenagers has declined over the past 10 to 15 years. Symptoms of mental illness have increased, as suicide rates have doubled for girls and increased by 50% for boys").

[297] *See e.g.*, *Generative AI Raises Competition Concerns*, FED. TRADE COMM'N (June 29, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns (observing how

The competitive value of user data can incentivize firms to prioritize acquiring it, even at the expense of user privacy and sometimes the law. Similarly, market concentration and market power can incentivize firms to deal with others on exclusionary terms or in ways that entrench and enhance their market position. Data abuse can raise entry barriers and fuel market dominance, and market dominance can, in turn, further enable data abuses and practices that harm consumers in an unvirtuous cycle. Meanwhile, the lack of competition can mean that firms are not competitively pressured to improve product quality with respect to privacy, data collection, and other service terms, such that users lack real choice and are forced to surrender to the data practices of a dominant company or a limited set of firms.

IX. Conclusion

The Companies' responses to the Commission's Order show that:

- The Companies' data practices posed risks to users' and non-users' data privacy and the Companies' data collection, minimization, and retention practices were inadequate.
- Many Companies relied on selling advertising services to other businesses, and much of this was based on using consumers' data to target ads. The technology powering this ecosystem took place behind the scenes and was largely out of view to consumers, but nonetheless posed privacy risks.
- There was a widespread application of Algorithms, Data Analytics, or AI to users' and non-users' data, which powered the SMVSSs—everything from content recommendation to search, advertising, and inferring personal details about users. But there were serious concerns with the ways the Companies used automated decision-making systems.
- Children and teens are a uniquely vulnerable population, but the Companies' policies have failed to adequately protect them—this is especially true of teens, who are not covered by the COPPA Rule.

This report's findings can, and should, inform decisions made by the public, policymakers, and companies with respect to SMVSSs.

---

access to data is an important input to training AI models, and in turn, to the provision of existing and emerging generative AI products).

Staff Recommendations

Based on this report's observations, findings, and analysis, staff make several recommendations, which are intended to inform decisions made by policymakers and companies regarding SMVSSs.[298]

1. Data Practices Recommendations

- **Congress should enact comprehensive federal privacy legislation that limits surveillance and grants consumers data rights.**[299] At a minimum, such comprehensive federal privacy legislation should grapple with the fact that protecting users' privacy requires addressing the business incentives that firms currently face, which often pit user privacy against monetization. Users should have baseline protections, such as default safeguards against the over-collection, monetization, disclosure, or undue retention of personal data. Users should be able to proactively choose whether they do or do not wish to be tracked, and they should be able to make this choice freely, rather than under conditions that restrict their autonomy. Users should also have the right to access the data collected from or about them and to delete data collected from or about them. Any comprehensive federal privacy legislation should also include a strong data minimization framework and require that SMVSSs maintain uniform and specific data retention and deletion practices, preventing them from keeping consumer data for any ambiguous and vague "business purpose."

- **Companies can and should do more to protect consumers' privacy.** SMVSSs can and should do more to protect consumer privacy, starting with this report's recommendations. However, it bears repeating that self-regulation is not the answer and federal legislation is necessary to ensure that the Companies protect consumers' privacy.

    - **SMVSSs should limit data collection.** SMVSSs should limit the data collected from both users and third parties to what is necessary for providing the service. Limited data collection will not only benefit the privacy of consumers, but also their security.[300]

---

[298] These recommendations are not intended to imply that a company's failure to follow them is necessarily an unfair or deceptive trade practice. Rather, the recommendations reflect staff's observations based on the documents received from the Companies as part of this study, along with staff's expertise and experience in these areas.

[299] The Commission first made a request for privacy-related legislation in 2000. *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE – A REPORT TO CONGRESS (May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf (stating that "the Commission recommends that Congress enact legislation to ensure adequate protection of consumer privacy online").

[300] *See, e.g.*, FED. TRADE COMM'N, START WITH SECURITY (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (stating that by only collecting the personal information that a business needs "[n]o one can steal what you don't have."); Thomas B. Pahl, *Start with security – and stick with it*, FED. TRADE COMM'N (July 28, 2017), https://www.ftc.gov/business-guidance/blog/2017/07/start-security-and-stick-it.

- **SMVSSs should limit data sharing with affiliates or company-branded entities.** SMVSSs should limit such data sharing, using it only for purposes that are necessary for providing the service a consumer is seeking. In addition, the lack of a delineated process and contractual language governing such data sharing may be appropriate for smaller companies with a smaller corporate footprint; however, where SMVSSs are part of multinational conglomerates, it would be prudent for them to establish and maintain thorough processes to oversee any and all sharing between affiliates and company-branded entities.

- **SMVSSs should limit data sharing with third parties.** SMVSSs should limit data sharing, using it only for purposes that are necessary for providing the service a consumer is seeking.

- **SMVSSs should implement more concrete and enforceable data minimization and retention policies.**

  - **Data Minimization**: SMVSSs should implement and maintain concrete written data minimization policies that impose limits keyed to what is reasonably necessary to provide the consumer's requested product or service, rather than allowing them to undertake any collection, use, or disclosure to monetize data.

  - **Data Retention:** SMVSSs should, in coordination with applying the recommended data minimization policies, develop, document, and adopt concrete data retention policies that include clear-cut and definite retention periods for each type of user data collected that are tied to the purposes for which the SMVSS collected the data.

- **SMVSSs should delete consumer data when it is no longer needed.** SMVSSs should properly delete consumer data when it is no longer needed rather than retaining the data in scrubbed format.

- **SMVSSs should adopt privacy policies that are clear, simple, and easily understood.** SMVSSs should adopt consumer-friendly privacy policies such that their average user can understand what the SMVSS's data collection practices are, including what data it collects, purposes for which the SMVSS collects the data, how long the SMVSS will keep that data, and any third parties to whom the SMVSS will disclose the data. Clear, simple, and plain-language notices are a key component of a robust privacy policy, though they do not substitute for strong substantive protections.

2. Advertising Recommendations[301]

- **Ad targeting restrictions, particularly restrictions based on sensitive categories, would benefit from greater clarity and consistency.** Ad targeting that is in any way based on sensitive categories can be distressing to users and result in a spectrum of harms. There was a lack of clarity and consistency regarding how the Companies described their ad targeting practices based on sensitive categories. This lack of clarity and consistency may be yet another reason why a comprehensive federal privacy law giving consumers control over their information is necessary. But companies should not wait for new laws to take action because discriminatory targeting can be illegal under existing laws, such as the Fair Housing Act. In light of this, we urge companies to carefully examine their policies and practices regarding targeting based on sensitive categories and to construe the categories of information considered to be sensitive broadly.

- **SMVSSs should not collect users' sensitive information via privacy-invasive ad tracking technologies.** Privacy-invasive tracking technologies such as pixels have the ability to transmit many types of information, including sensitive information about users' actions to SMVSSs that use them. Advertisers need to exercise caution when deploying such tracking technologies so that they do not collect sensitive information. And, SMVSSs that receive sensitive information for advertising or marketing purposes should take steps to prevent the receipt, use, or onward disclosure of sensitive information. Indeed, the alleged failure to do so has already subjected some firms to legal challenges,[302] and, depending on the facts, the recipients of such data could also face liability under Section 5.[303]

3. Algorithms, Data Analytics, and AI Recommendations

- **Companies should address the lack of access, choice, control, transparency, explainability, and interpretability relating to their use of automated systems**. Users and non-users could not control whether or how their Personal Information was used by Algorithms, Data Analytics, or AI in the first place, and there was limited or no ability to opt in to or opt out of such uses. In fact, users might not even be aware of the ways in which their information was processed by automated systems. Nor were users and non-users empowered to review the information used by these systems or their outcomes, to correct incorrect data or determinations, or to understand how the decisions were made.

---

[301] Policymakers should recognize that incremental efforts to limit invasive targeting practices are unlikely to suffice when business models are built on such practices.

[302] *See, e.g., Hodges, et al. v. GoodRx Holdings Inc.*, Case No. 1:23-cv-24127-BB (S.D. Fla. 2023); *Doe v. Meta Platforms, Inc.*, Case No. 3:22-cv-03580-WHO (N.D. Cal. 2023).

[303] *See, e.g.,* Elisa Jillson, *Protecting the Privacy of Health Information: A Baker's Dozen Takeaways from FTC Cases*, FED. TRADE COMM'N (July 2023), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases.

- **Companies should implement more stringent testing and monitoring standards.**[304] The Companies had varying policies relating to testing and monitoring their use of automated systems, with some Companies having fewer or lacking sufficient policies or practices to monitor and test for things such as unlawful discrimination. Companies offered differing and sometimes vague descriptions of their human review, monitoring, testing capabilities, and frequency of testing, which also raises a host of risks and concerns. There also was generally a lack of testing and auditing of automated systems by independent third parties. Companies should do more to ensure their testing and monitoring of automated systems is rigorous, comprehensive, and consistent. This wide-ranging and ubiquitous reliance on automated systems, mixed with sometimes limited, inconsistent, or differing human review, oversight, or testing practices poses risks for consumers and society.

- **Legislation and regulation are badly needed.** It is clear that when it comes to ensuring these firms' AI systems do not result in unlawful discrimination, error, addiction, and other harms, self-regulation is failing. In particular, rules that set forth clear guardrails for the responsible use of automated systems are overdue. The Companies' differing, inconsistent, and sometimes inadequate approaches to monitoring and testing is one example of why robust regulatory tools and radically more transparency are needed. Although the FTC has made clear how Section 5 applies to the harmful use of AI, comprehensive federal legislation would cement baseline consumer data rights and protections and ensure that there are additional powerful regulatory and enforcement tools to combat challenges head on.[305] In the absence of comprehensive efforts to combat potential harms, such as unlawful bias, these automated tools and systems can serve to further entrench pre-existing inequalities and invade consumers' privacy.

4. Children and Teen Recommendations

- **COPPA should be the floor, not the ceiling.** SMVSSs should view the COPPA Rule as representing the minimum requirements and provide additional safety measures for Children as appropriate.

- **The SMVSSs should not ignore the reality that there are Child users.** Willfully ignoring a Child user on their SMVSSs will not help companies avoid liability under COPPA. Moreover, for those SMVSSs that do not permit Child users, they should design, implement and maintain more definitive policies regarding what they would do when (not if) a Child user is discovered on their service.

---

[304] This report and its recommendations do not address or endorse any attempt to censor or moderate content based on political views.

[305] Even in the absence of comprehensive federal legislation, several federal agencies are using their existing legal authorities and applying them to the use of automated systems and AI just as they apply to other practices. These agencies include the Federal Trade Commission, Department of Justice, Equal Employment Opportunity Commission, the Consumer Financial Protection Bureau, Department of Housing and Urban Development, Department of Health and Human Services, Department of Education, Department of Homeland Security, and Department of Labor. *See supra* note 224.

- **SMVSSs should provide parents/legal guardians an easy way to manage their Child's Personal Information.** SMVSSs should provide a uniform, easy, and straightforward process by which parents/legal guardians can request access to, or deletion of, any Personal Information collected from their Child.

- **SMVSSs should do more to protect Teen users of their services.** SMVSSs are failing to adequately to protect Teen users. The SMVSSs should recognize that Teen users are not adult users and, at a minimum, should do the following: (1) design age-appropriate experiences for Teen users; (2) afford Teen users the most privacy-protective settings by default; (3) limit the collection, use, and sharing, of Teen users' data; and (4) only retain Teen users' personal information for as long as necessary to fulfill the purpose for which it was collected.[306]

- **Congress should enact federal privacy legislation that protects Teen users online.** As previously discussed, COPPA applies only to Children. This results in a gap wherein society does not recognize Teens as adults, but there is no legislation afforded to protect Teens' privacy in the digital world. For many reasons, including those discussed in this report, Teens should be afforded legal rights and protections that take into account the unique harms posed to Teens online and the significant developmental changes Teens undergo.

5. Competition Recommendations

- **Antitrust enforcers should carefully scrutinize potential anticompetitive acquisitions and conduct.** Antitrust enforcers should consider the effects of unlawful acquisitions and conduct on competition and consumers, including how companies treat consumers with respect to data, privacy, and AI, and the competitive implications of these practices.

- **The foregoing staff recommendations could also promote competition.** The other recommendations described above could both provide direct benefits to consumers and promote healthy competition. For instance, requiring companies to be more transparent regarding their data, privacy, and automated decision-making practices would arm consumers with better information, allowing new or existing firms to compete with large incumbent SMVSSs more readily by distinguishing themselves regarding these practices. In addition, enforcers should remain vigilant in evaluating the business incentives driving firm conduct to ensure consumer choice, fair dealing, and robust competition in online service markets.

---

[306] Such recommendations come from the Kids Online and Safety Task Force report that FTC Commissioner Alvaro Bedoya signed onto. *See* KIDS ONLINE HEALTH & SAFETY TASK FORCE, ONLINE HEALTH AND SAFETY FOR CHILDREN AND YOUTH: BEST PRACTICES FOR FAMILIES AND GUIDANCE FOR INDUSTRY (July 2024), https://www.samhsa.gov/sites/default/files/online-health-safety-children-youth-report.pdf.

Appendix A:
Copy of Order

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS:	**Joseph J. Simons, Chairman**
	Noah Joshua Phillips
	Rohit Chopra
	Rebecca Kelly Slaughter
	Christine S. Wilson
FTC Matter No.	**P205402**

ORDER TO FILE A SPECIAL REPORT

Pursuant to a resolution of the Federal Trade Commission ("FTC" or "the Commission") dated December 11, 2020, entitled "Resolution Directing Use of Compulsory Process to Collect Information Regarding Social Media and Video Streaming Service Providers' Privacy Practices," a copy of which is enclosed, **[COMPANY NAME],** hereinafter referred to as the "Company," is ordered to file with the Commission, no later than 45 days after date of service, a Special Report containing the information and Documents specified herein.

The Commission is seeking information concerning the privacy policies, procedures, and practices of Social Media and Video Streaming Service providers, Including the method and manner in which they collect, use, store, and disclose Personal Information about consumers and their devices. The Special Report will assist the Commission in conducting a study of such policies, practices, and procedures.

The Special Report is required to be subscribed and sworn by an official of the Company who has prepared or supervised the preparation of the report from books, records, correspondence, and other data and material in Your possession. Your written report should restate each item of this Order with which the corresponding answer is Identified. If any question cannot be answered fully, give the information that is available and explain in what respects and why the answer is incomplete. The Special Report and all accompanying documentary responses must be Bates-stamped.

You are required to respond to this Order using information in Your possession, custody, or control, Including information maintained in a central data repository to which You have access. You should not seek any responsive information and data from separately incorporated subsidiaries or affiliates or from individuals (other than in their capacity as Your employee or as Your agent). However, You should provide information from separately incorporated subsidiaries or affiliates or from individuals if You already have possession, custody, or control of such information. No later than 14 days from the date of service, You should contact Commission staff and indicate whether all of the information required to respond to this Order is in Your possession, custody, or control. If certain information is not in Your possession, custody, or control, no later than 14 days from the date of service, You also must: (1) Identify, both orally and in writing, each question or sub-question that You are not able to fully answer because information is not in Your possession, custody, or control, and (2) for each, provide the

full names and addresses of all entities or individuals who have possession, custody, or control of such missing information.

Confidential or privileged commercial or financial information will be reported by the Commission on an aggregate or anonymous basis, consistent with Sections 6(f) and 21(d) of the FTC Act. Individual submissions responsive to this Order that are marked "confidential" will not be disclosed without first giving the Company ten (10) days' notice of the Commission's intention to do so, except as provided in Sections 6(f) and 21 of the FTC Act.

SPECIFICATIONS

Please produce the following information, Documents, and items, consistent with the definitions, instructions, and formatting requirements contained in Attachment A.

Identification of Report Author

1. Identify by full name, business address, telephone number, and official capacity the individual(s) who prepared or supervised the preparation of the Company's response to this Order, and Describe in Detail the steps taken by the Company to respond to this Order. For each Specification, Identify the individual(s) who assisted in preparation of the response. Produce a list Identifying the individual(s) whose files were searched, and Identify the individual(s) who conducted the search.

Company Information

2. State the Company's complete legal name and all other names under which it has done business, its corporate mailing address, all addresses from which it does or has done business, and the dates and states of its incorporation.

3. Describe the Company's corporate structure, and state the names of all parents, subsidiaries, divisions, affiliates, branches, joint ventures, franchises, operations under assumed names, websites, and entities over which it exercises supervision or control. For each such entity, Describe in Detail the nature of its relationship to the Company and the date it was created, acquired, sold, or otherwise changed ownership or control. Produce organizational charts sufficient to detail the Company's corporate structure.

4. If the Company is not publicly traded, Identify each individual or entity having an ownership interest in the Company, as well as their individual ownership stakes and their positions and responsibilities within the Company.

General Information Regarding Social Media and Video Streaming Services

5. Identify each Social Media and Video Streaming Service provided or sold by the Company from January 1, 2019 to the present in each Relevant Area, and for each such Social Media and Video Streaming Service, separately for all users in total and for each mutually exclusive Selected User Group, provide, on a monthly basis, separately for

desktop and mobile, the number of users and the value of each User Metric, in total and on average per monthly active user (if applicable), Including:

a) number of registered users;

b) daily active users ("DAUs");

c) monthly active users ("MAUs");

d) time spent;

e) number of sessions;

f) unique posts, separately by photos, videos, stories, or other;

g) views, separately by photos, videos, stories, or other;

h) "like" or "recommend" actions (e.g., likes, upvotes, downvotes);

i) shares, reposts, or forwards, within the Social Media and Video Streaming Service or to any other Social Media and Video Streaming Service;

j) comments;

k) messages sent, separately by text, video, and image messages;

l) status updates;

m) size of the social graph;

n) User Network Size;

o) privacy settings;

p) User Engagement on any Social Media and Video Streaming Service, or other product or service, owned by any Person other than the Company;

q) value of user to the Company (e.g., dollar value);

r) exposure to ads (e.g., ad load);

s) ad engagement;

t) ads viewed for (i) each Advertising Format and (ii) all Advertising Formats in total;

u) ads viewed for (i) each Advertising Format and (ii) all Advertising Formats in total; as a share of total posts, stories, and messages viewed; and

v) any other measure of user traffic, density, engagement, or activity used by the Company in the ordinary course of business.

Provide with Your response a description of each User Metric, Including a description of how each User Metric is calculated, and a data dictionary with each such metric.

Submit a list of available mutually exclusive Selected User Groups to Commission counsel before submitting a full response to Specification 5. If the Company lacks a value (e.g., "yes," and "no," for whether a natural Person is of Hispanic, Latino or Spanish origin) for a Selected User Attribute for any user, the Company should treat "missing" as the value of that Selected User Attribute for the users who lack a value.

For the limited purpose of illustrating the concept of mutually exclusive Selected User Groups, assume that the Selected User Attributes are age, whether a natural Person is of Hispanic, Latino or Spanish origin, and country, and that the mutually exclusive values for those Selected User Attributes are 0-25 years, 26-50 years, 50+ years, and "missing" for age; yes, no and "missing" for whether a natural Person is of Hispanic, Latino or Spanish origin; and United States, Other, and "missing" for country. The number of mutually exclusive Selected User Groups in the Company's response would be the product of the number of mutually exclusive values for each Selected User Attribute: N = (# of age values)*(# of origin values)*(# of country values).

In this example, the Company's response would Include 36 mutually exclusive Selected User Groups per month [(4 age values)*(3 origin values)*(3 country values) = 36], and the Company's response should Include the number of registered users in each such group and the value of each User Metric, on a monthly basis, in total and on average per MAU (if applicable), for each such group of users. The spreadsheet in Appendix A illustrates this example.

6. For each Social Media and Video Streaming Service identified in response to Specification 5, provide, on a monthly basis, separately for each Relevant Area, the total number of registered users and value of each User Metric, in total and on average per MAU (if applicable), separately for the subset of users in each Selected User Group that were:

   a) MAUs on such Social Media and Video Streaming Service; and

   b) MAUs on such Social Media and Video Streaming Service and also active on another Social Media and Video Streaming Service provided or sold by any Person other than the Company, stated separately for each other Social Media and Video Streaming Service (and Identifying such other Social Media and Video Streaming Service).

7. For each Social Media and Video Streaming Service identified in response to Specification 5, separately for each Relevant Area, Identify and describe each metric (Including the inputs and the methodology used to calculate the metric) that the Company uses to assess the service's penetration or reach (e.g., 1-day reach, 30-day reach, installed base, or app downloads). Provide each such metric (Including the inputs used to

calculate the metric) on a monthly basis, stated separately for each Social Media and Video Streaming Service in each Relevant Area.

8. For each Social Media and Video Streaming Service identified in response to Specification 5, separately for each Relevant Area, state, on a monthly, quarterly, and annual basis:

   a) the Company's revenue, other than advertising revenue, stated in dollars, stated separately by type of revenue, Including gross and net revenue;

   b) the Company's revenue for each Digital Advertising Service on the Social Media and Video Streaming Service, stated in dollars, stated separately by type of revenue, Including gross and net revenue;

   c) the Company's costs and expenses, other than for Digital Advertising Services on the Social Media and Video Streaming Service, stated in dollars, Including, but not limited to, cost of revenue, traffic acquisition costs, and revenue guarantees;

   d) the Company's costs and expenses for each Digital Advertising Service on the Social Media and Video Streaming Service, stated in dollars, Including, but not limited to, cost of revenue, traffic acquisition costs, and revenue guarantees;

   e) the Company's prices for revenue-generating products or services other than advertising revenue; and

   f) the Company's gross margins, operating margins, and the method of computation.

9. State whether the Company uses data professionals (e.g., a privacy engineer) in the management and operation of its Social Media and Video Streaming Service's privacy, ethics, or bias efforts, and state their roles (e.g., legal, technical, operational, design, etc.) in the Social Media and Video Streaming Service's product lifecycle, Including any privacy, bias, or ethics-focused professionals working on Algorithms or Data Analytics utilized by a Social Media and Video Streaming Service, and Describe in Detail their responsibilities.

Data Collection, Use, Storage, Disclosure, and Deletion

10. For each Social Media and Video Streaming Service identified in response to Specification 5, separately for each Relevant Area, Identify each User Attribute that the Company uses, tracks, estimates, or derives, Including, but not limited to, each User Attribute Related to the Company's sale of Digital Advertising Services such as User Attributes for targeted advertising. Further, provide the following:

    a) For each such User Attribute, Identify and provide the available values for that attribute (e.g., "yes," "no" for whether the natural Person is of Hispanic, Latino, or Spanish origin) that the Company uses, tracks, estimates, or derives.

b) For each Social Media and Video Streaming Service in each Relevant Area, Identify, on an annual basis, the top 1,000 most populous User Attribute values (excluding "missing" as a value), based on average number of MAUs of the Social Media and Video Streaming Service, and for each, provide, on an annual basis:

i) the number of registered users;

ii) the average number of DAUs;

iii) the average number of MAUs;

iv) the total time spent;

v) the average time spent per day per MAU; and

vi) the average value of the user to the Company, Including average revenue per user.

c) For each Social Media and Video Streaming Service in each Relevant Area, Identify, on an annual basis, the top 1,000 User Attribute values most frequently used by the Company and advertisers on the Company's Social Media and Video Streaming Service to target advertising or match advertisements to users, provide a description of the Company's criteria and method for determining the top values, and, for each top value, provide, on an annual basis:

i) the number of registered users;

ii) the average number of DAUs;

iii) the average number of MAUs;

iv) the total time spent;

v) the average time spent per day per MAU; and

vi) the average value of the user to the Company, Including average revenue per user.

d) Identify any metric the Company uses, tracks, estimates, or derives to assess the accuracy of its User Attribute information, and, for each such metric, provide on an annual basis, the value of each such metric.

11. Describe in Detail the process for Identifying and reporting inaccurate User Attribute information, and the process, if any, for remedying any harms caused by these inaccuracies, Including all oversight provided by senior leadership as identified by position. For each Social Media and Video Streaming Service in each Relevant Area, Identify, on an annual basis:

a) the number of inaccurate User Attributes identified per quarter;

b) the top 100 types of inaccuracies (e.g., fake account, unauthorized account, bot, inaccurate information, invalid clicks or views, etc.) and their primary genesis if known;

c) the top 1,000 User Attributes with inaccuracies in rank order, starting with the attribute with the most inaccuracies;

d) the number and type of advertisements shown based on (i) inaccurate information overall, (ii) top 1,000 User Attributes with inaccuracies, and (iii) for each of the top 100 types of inaccuracies where applicable;

e) the total and average cost of advertisements placed based on (i) inaccurate information overall, (ii) top 1,000 User Attributes with inaccuracies, and (iii) for each of the top 100 types of inaccuracies where applicable;

f) the total and average revenue value, Including but not limited to revenue derived from (i) inaccuracy overall, (ii) top 1,000 User Attributes with inaccuracies, and (iii) for each of the top 100 types of inaccuracies where applicable; and

g) the total and average amount of restitution provided to third parties harmed by (i) inaccuracy overall, (ii) for the top 1,000 User Attributes with inaccuracies, and (iii) for each of the top 100 types of inaccuracies where applicable.

12. For each Social Media and Video Streaming Service identified in response to Specification 5, submit all Documents Relating to the Company's or any other Person's strategies or plans, Including, but not limited to:

a) business strategies or plans;

b) short-term and long-range strategies and objectives;

c) expansion or retrenchment strategies or plans;

d) research and development efforts;

e) sales and marketing strategies or plans, Including, but not limited to, strategies or plans to expand the Company's customer base or increase sales and marketing to particular customer segments (e.g., a user demographic);

f) strategies or plans to reduce costs, improve products or services (e.g., expanding features or functionality), or otherwise become more competitive;

g) plans to enter into or exit from the sale or provision of any Relevant Product or other product or service;

h) presentations to management committees, executive committees, and boards of directors; and

i) budgets and financial projections. For regularly prepared budgets and financial projections, the Company need only submit one copy of final year-end Documents for prior years, and cumulative year-to-date Documents for the current year.

13. For each Social Media and Video Streaming Service identified in response to Specification 5, submit all Documents Relating to the Company's or any other Person's advertising or premium subscription pricing plans, pricing strategy, pricing practices, pricing decisions, pricing Analyses, and pricing policies, Including, but not limited to, pricing Algorithms or Data Analytics, discount policies, pricing programs, and bundling strategies.

14. Describe in Detail how the Company shares users' and non-users' Personal Information with, or obtains users' and non-users' Personal Information from, its affiliates or other Company-branded entities. As part of Your response, (a) Identify those entities and Describe in Detail the types of Personal Information and purposes for such sharing or obtaining; and (b) Describe in Detail and provide any policies or contracts detailing sharing and use restrictions among affiliates and Company-branded entities.

15. Describe in Detail how the Company shares users' and non-users' Personal Information with, or obtains users' and non-users' Personal Information from, third parties. As part of Your response, (a) Identify those entities and Describe in Detail the types of Personal Information and purposes for such sharing or obtaining; and (b) Describe in Detail and provide any policies or contracts applicable to such sharing.

16. Describe in Detail how the Company collects, assembles, purchases, or otherwise obtains information Related to a consumer's shopping behavior, Including at offline and online retail outlets (e.g., grocery stores). Include in Your response a detailed description of how the Company uses this data, or permits this data to be used, to target individual consumers or members of a household.

17. Submit all data deletion and retention policies the Company has in place. If the Company does not have such data deletion and retention policies, Describe in Detail the Company's data deletion and retention practices, Including (a) any retention periods for Personal Information collected from or about users and their devices, or information inferred about users and their devices; (b) how these practices apply to Personal Information associated with canceled or abandoned accounts; and (c) the process for responding to a third party request to delete data.

18. Describe in Detail the Company's policies and procedures Related to the minimization of Personal Information, as well as policies and procedures to ensure that the Company's employees, affiliates, and third parties with whom the Company shares such Personal Information comply with these policies and procedures.

19. Describe in Detail any analyses the Company performed on different variations of user interfaces for users' privacy settings or ability to exercise access, correction, porting, or deletion rights. Produce the Documents associated with and all results of such Analyses. Describe in Detail any changes to the user interfaces as a result of these processes, the

dates these changes were made, and every metric and its value pertaining to the financial, growth, or other Company outcomes associated with each change. State, separately for each month from January 1, 2019 onward, the number of users who (a) made changes to their privacy settings; (b) requested access to their data; (c) requested correction of their data; (d) requested to port their data; or (e) requested to delete their data. If any of these choices were not honored, Describe in Detail why.

20. For each Social Media and Video Streaming Service identified in response to Specification 5, Describe in Detail how academics and researchers may request access to Personal Information or other information held by the Social Media and Video Streaming Service, and what types of Personal Information and other information such academics and researchers may access. Produce all materially different contracts or policies that apply to academics' and researchers' use of Personal Information or other information.

Advertising

21. Identify each Digital Advertising Service sold or provided by the Company from January 1, 2019 to the present in each Relevant Area, and for each such service, provide the following information:

    a) a description of the Digital Advertising Service;

    b) its intended user or user segment;

    c) whether the product or service is priced by cost-per-click, cost-per-impression, revenue split, or other formula;

    d) whether the intended focus of the product or service is for brand awareness advertising, performance advertising, product purchase, or other purposes; and

    e) the targeting capabilities of the product or service, Including, but not limited to, a description of all data points that can be used to target (e.g., user information, mobile device type, location information, application being used, keywords), and the source of that data.

22. For each Digital Advertising Service identified in response to Specification 21, separately for each Relevant Area, state on a monthly, quarterly, and annual basis:

    a) the Company's revenue, other than those for advertising on any Social Media and Video Streaming Service reported in Specification 8(b), stated in dollars, Including, but not limited to, gross revenue, separated by advertising and non-advertising revenues; and

    b) the Company's costs and expenses, other than those for advertising on any Social Media and Video Streaming Service reported in Specification 8(d), stated in dollars, Including, but not limited to, cost of revenue, traffic acquisition costs, or revenue guarantees, exclusive of the costs and expenses reported in response to Specification 8(d); and

c) the Company's gross margins, operating margins, and the method of computation.

23. For each Digital Advertising Service identified in response to Specification 21 separately for each Relevant Area, Identify and describe (Including, but not limited to, describing how the Company defines each item in the ordinary course):

a) each Advertiser Metric, Including but not limited to, each metric for:

i) ad revenue;

ii) number of bids in auctions that resulted in an ad being shown to a user;

iii) number of advertisers;

iv) number of impressions (i.e., ads shown to a user);

v) number of clicks;

vi) click-through rate (i.e., number of clicks per impression);

vii) measures of User Engagement (e.g., number or users or average time spent per user);

viii) average winning advertiser bid for ads shown to a user;

ix) average price determined by the auction for ads shown to a user (e.g., average cost per click or cost per action);

x) average cost per mille (i.e., cost per thousand impressions) regardless of whether cost to advertisers was based on number of views or other user actions;

xi) number of ads shown to a user that resulted in the desired Advertising Objective (e.g., conversions);

xii) advertiser return on investment (e.g., return on ad spend); and

xiii) the existence or absence of other advertising Publishers and their identities;

b) each Advertising Objective;

c) the pricing models available for each Advertising Objective (e.g., cost per click or cost per impression);

d) each Selected Advertiser Attribute, and each mutually exclusive value for each such Selected Advertiser Attribute (e.g., "small business" or "large business" for advertiser size) tracked by, derived by, estimated by, or available to the Company (with "missing" treated as a value if the Company lacks a value for the Advertiser Attribute for every advertiser);

e) each mutually exclusive Selected Advertiser Category (i.e., each mutually exclusive group of advertisers reflecting each mutually exclusive combination of Selected Advertiser Attribute values), and each set of Selected Advertiser Attribute values used to define such Selected Advertiser Category; and

f) each Advertiser Metric the Company provided to any other Person and the time periods for which such information was provided, stated separately for each Third-Party Category, Including, but not limited to, app developers, analytics partners, and advertisers.

24. For each Digital Advertising Service, (i) by Advertising Placement, (ii) by Country Location where the advertisement was displayed, (iii) by Advertising Format, (iv) by each pricing model available for Advertising Objectives, (v) by whether sales are direct or by auction, (vi) by desktop and by mobile; provide, on a monthly basis, the number of advertisers and the value of each Advertiser Metric identified in response to Specification 23(a), for:

a) all advertisers in total; and

b) each mutually exclusive Selected Advertiser Category.

Provide with Your response a description of each Advertiser Metric, Including a description of how each Advertiser Metric is calculated, and a data dictionary with each such metric.

Submit a list of available mutually exclusive Selected Advertiser Categories to Commission counsel before submitting a full response to Specification 24. If the Company lacks a value for a Selected Advertiser Attribute for any advertiser, the Company should treat "missing" as the value of that Selected Advertiser Attribute for the advertisers who lack a value.

For the limited purpose of illustrating Specification 24(b), assume that the Selected Advertiser Attributes are advertiser size, industry vertical, and spend tier, and that the mutually exclusive values for those Selected Advertiser Attributes are small business, large business, and "missing" for advertiser size; ecommerce, gaming, and "missing" for industry vertical; and "1" and "2" for spend tier. The number of mutually exclusive Selected Advertiser Categories in the Company's response would be the product of the number of mutually exclusive values for each Selected Advertiser Attribute: N = (# of advertiser size values)*(# of industry vertical values)*(# of spend tier values).

In this example, the Company's response would Include 18 mutually exclusive Selected Advertiser Categories per month [(3 advertiser size values)*(3 industry vertical values)*(2 spend tier values) = 18], and the Company's response should Include the number of advertisers in each such group and the value of each Advertiser Metric, on a monthly basis, for each such group of advertisers. The spreadsheet in Appendix B illustrates this example.

25. For each Digital Advertising Service:

a) Identify, on a monthly basis:

i) the top 100 advertisers in each mutually exclusive Selected Advertiser Category, by revenue generated by the Company on advertisements displayed in the United States; and

ii) the top 100 advertisers in each mutually exclusive Selected Advertiser Category, by revenue generated by the Company on advertisements displayed worldwide; and

b) for each such advertiser and month identified in subparts (a)(i) and (a)(ii), provide:

i) the value of each Selected Advertiser Attribute for the advertiser; and

ii) the ad revenue in the relevant geography for the advertiser by (1) Advertising Format, (2) each pricing model available for Advertising Objectives, (3) whether advertising purchases are direct or by auction, and (4) desktop and mobile.

26. Submit all Documents Relating to the sale or provision of any Digital Advertising Service or the display of advertising to users in any Relevant Area, Including, but not limited to, all Documents Relating to:

a) the Company's collection of, or access to, information about user or consumer activities, attributes, or interests;

b) the tracking of user or consumer activity on or off of the Company's products or services;

c) the quality or accuracy of the Company's measurement or assessment of user activities, attributes, and interests, and the Company's ability to target advertising;

d) the effect of advertising, Including advertising load, on consumer behavior or user activity, engagement, growth, retention, or attrition; and

e) the effect of advertising load and advertising inventory volume on revenue, price, and profitability of the Company's Digital Advertising Services.

Algorithms or Data Analytics

27. For each Social Media and Video Streaming Service identified in response to Specification 5, state whether the Social Media and Video Streaming Service applies Algorithms or Data Analytics to Personal Information, and if so, Describe in Detail the specific categories of Personal Information to which the Algorithms or Data Analytics are applied and each of the ways the Company uses Algorithms or Data Analytics, Including:

a) the processes and techniques used:

i) to prepare data for Analysis, Including but not limited to locating, acquiring, and ingesting data; assessing and cleaning data; reconciling and making data uniform; extracting, restricting, and linking data; coding and annotating data; and updating data as new information becomes available; and

ii) to analyze data, Including but not limited to:

(1) descriptive and exploratory Analysis;

(2) predictive Analysis, such as machine learning, linear regression, non-linear regression classification, data mining, text analytics, Bayesian methods, and simulation; and

(3) prescriptive Analysis, such as stochastic models, and optimization;

b) the sources of such Personal Information, Including

i) whether the source is the user, affiliate, third party or other, and if other, describe;

ii) the top 100 non-user sources of data;

iii) categories of data procured on existing users, uses for each category, the total cost and average cost per user for each category from each source, and the total value both overall and per user, Including revenue, derived from each category, per source and per use;

iv) categories of third-party data procured on nonusers, uses for each category, the total cost and average cost per user for each category from each source, and the total value both overall and per user, Including revenue, derived from each category, per source and per use; and

v) the processes and techniques used to integrate or otherwise monetize data from each third-party source, any new predictive capability or other Company outcome enabled by each integration, and the value, Including revenue, derived from any integration, predictive capability, and/or other Company use of external data;

c) the purpose(s) for which the Company applies Algorithms or Data Analytics to the Personal Information, Including but not limited to:

i) to make inferences or conclusions, and if so, the types of inferences and conclusions the Company makes; and

ii) to make decisions, and if so, the types of decisions the Company makes;

d) whether the Social Media and Video Streaming Service has any written policies and procedures with respect to the development or application of Algorithms or Data Analytics to Personal Information. If so, produce such policies and procedures; and

e) whether the Social Media and Video Streaming Service monetizes the development or application of such Algorithms or Data Analytics to the Personal Information, and if so, how the Company monetizes such applications (i.e., research and development, third-party sales, etc.).

28. For each Social Media and Video Streaming Service that applies Algorithms or Data Analytics to Personal Information identified in response to Specification 27, Describe in Detail how the Company identifies and addresses privacy, security, or ethics issues with respect to the application of Algorithms or Data Analytics to Personal Information, Including:

a) the Company's use of Classifiers, Including (i) how often Classifiers are revised, considered, and retrained; and (ii) whether it excludes or limits use of any Classifiers;

b) whether the Company examines whether data sets are missing information from particular populations, and if so, how the Company examines data sets for missing information from particular populations and what steps it takes to address such missing information; and

c) whether the Company examines any correlations and other empirical relationships found by the application of Algorithms or Data Analytics, and if so, how the Company determines whether the correlations and empirical relationships are meaningful.

29. For each Social Media and Video Streaming Service that applies Algorithms or Data Analytics to Personal Information identified in response to Specification 27, Describe in Detail how the Company monitors and tests the application of Algorithms or Data Analytics to Personal Information, Including:

a) the Person(s) responsible for monitoring and testing the Algorithms or Data Analytics;

b) the process(es) by which the Company monitors and tests the accuracy or impact of the Algorithms or Data Analytics, Including the extent to which the processes are automated or rely on human intervention;

c) the frequency with which the Company tests, validates, and reviews the accuracy or impact of any Algorithms or Data Analytics;

d) whether the Company determines that any decisions made by Algorithms or Data Analytics are reliable, and if so, how the Company determines that any decisions made by Algorithms or Data Analytics are reliable;

e) how the Company determines the accuracy of any decisions made by the Algorithms or Data Analytics, Including the false-positive and false-negative rates;

f) whether the Company examines or tests data sets and Algorithms for bias, or allows affiliates or third parties to examine or test for bias, and if so how the Company, affiliates, or third parties examine and test data sets and Algorithms for bias, Including which types of demographic categories the Company, affiliates, or third parties analyze, and, if the Company or third party finds bias, the steps the Company takes to address it;

g) how the Company monitors any automated decision-making by the Algorithms or Data Analytics;

h) how the Company evaluates the usefulness of any particular Algorithm or Data Analytics; and

i) the frequency with which the Company updates or modifies its Algorithms or Data Analytics.

30. Produce all relevant policies and procedures, and any Analysis associated with evaluating, monitoring, testing, and validating the use or application of Algorithms or Data Analytics to Personal Information.

31. Describe in Detail how the Company uses Algorithms or Data Analytics to sell or provide any Digital Advertising Service or display advertising to users. Your response should Describe in Detail the process for and the frequency of updates to Algorithms or Data Analytics to remove inaccurate or unauthorized information (Including information on Children and Teens, or information retained after a user revokes consent), and information that users deleted. Produce Documents sufficient to show all:

a) Analyses of each such update, remedial actions taken following each such update, and/or strategies and rationale on timing of updates; and

b) Analyses of financial metrics associated with each such update, remedial actions taken following each such update, and/or strategies and rationale on timing of updates.

User Engagement

32. For each Social Media and Video Streaming Service identified in response to Specification 5, Describe in Detail how the Company measures, promotes, and researches User Engagement, Including:

a) tools the company uses, Including but not limited to Algorithms or Data Analytics, to increase User Engagement;

b) how the Company studies and analyzes User Engagement, Including User Engagement with other products and services offered by the Company or User Engagement's impact on advertising revenue; and

c) how a user's negative interactions with the Social Media and Video Streaming Service (e.g., blocking or unsubscribing from content) affect the user's engagement.

33. For each Social Media and Video Streaming Service identified in response to Specification 5, Describe in Detail what factors influence what content (whether user-created or ad-based) users see in the Social Media and Video Streaming Service, Including:

a) how the Company moderates content;

b) how the Company targets, surfaces, or promotes content;

c) what ranks and measures, Including if applicable User Attributes, the Company uses to target, surface, or promote content to users;

d) whether the display of information differs if a user is logged in or logged out of an application or service; and

e) how user-created content presentation is influenced by, impacted by, or in any way associated with the Company's advertising goals and outcomes.

34. For each Social Media and Video Streaming Service identified in response to Specification 5, separately for each Relevant Area, Identify each rank, measure, or User Attribute that the Company uses, tracks, estimates, or derives, to target, surface, or promote content to users. Additionally, Identify the top values most heavily weighted by the Company in order to target content or surface or promote user-created content. If You provided this information in response to Specification 10 or Specification 32, please Identify the relevant information.

35. For each Social Media and Video Streaming Service identified in response to Specification 5, submit all of the Company's content moderation policies and content promotion policies.

36. For each Social Media and Video Streaming Service identified in response to Specification 5, submit Documents sufficient to show the Company's development, launch, growth, performance, termination, or discontinuance of any User Engagement strategy or Social Media and Video Streaming Service strategy for targeting, surfacing, or promoting user content, Including but not limited to:

a) any efforts, strategies, or tools of the Company to increase the number of users or User Engagement;

b) any efforts, strategies, or tools of the Company to develop new or improved features or functionality; and

c) any action or decision of the Company to terminate or discontinue any Social Media and Video Streaming Service offering or functionality.

37. Provide representative samples of each type of promotional material the Company disseminates referring or Relating to User Engagement, Including revenue derived from such User Engagement.

38. Describe in Detail any strategies, efforts, processes, plans, and/or presentations associated with producing higher revenue, generating growth, spurring User Engagement, or soliciting user agreement by making changes to user interfaces or designs, and the outcomes and/or metrics associated with any changes made to user interfaces or designs. To the extent Your responses to Specifications 12 or 17 Include this information, Identify the relevant information.

Demographic Information

39. For each Social Media and Video Streaming Service identified in response to Specification 5, Describe in Detail the types of Demographic Information, Including how the Company categorizes this information (e.g., Hispanic/non-Hispanic) it collects, infers, or otherwise processes about (a) users, (b) their households, (c) non-users, and (d) their households.

40. Describe in Detail how the Company identifies, predicts, determines, infers, or makes correlations with or about Demographic Information, Familial Status, or Familial Relationships, Including based on:

a) content a user posts on or shares with the Social Media and Video Streaming Service;

b) Algorithms or Data Analytics;

c) Personal Information, Including whether and how the Company uses location data (whether or not such data is associated with other identifiers or other data) for such purposes; and

d) content engagement (e.g., clicking on specific ads, joining groups, attending events, liking or following specific brands).

41. Describe in Detail all the Company's uses of Demographic Information, Familial Status, or Familial Relationships, Including:

a) how the Company uses Demographic Information, Familial Status, or Familial Relationships for ad targeting or exclusions;

b) if the Company personalizes content based on Demographic Information, Describe in Detail all content and design features that are personalized, the purpose of personalizing (e.g., User Engagement, convenience, advertising, implementing choices, data Analysis, classification into segments, in-gaming content modification,

etc.), and what Demographic Information the Company uses to personalize those features;

c) how the Company uses such information in connection with lookalike modeling, and Describe in Detail whether and, if so, how the Company uses or avoids selecting protected characteristics for this process. Produce a representative list of all characteristics the Company offers for lookalike modeling; and

d) Identify the top five entities (by amount of revenue generated) with whom the Company has contracts that engage in or facilitate programmatic marketing (Including real-time bidding, guaranteed direct buying, and preferred deals) for advertising space on the Company's Social Media and Video Streaming Service(s).

42. For each Social Media and Video Streaming Service identified in response to Specification 5, Describe in Detail what mechanisms, if any, users and non-users have to inquire about or request access or deletion of the Demographic Information the Company has collected, and provide all user interfaces for such requests or inquiries. Describe in Detail policies, practices, and procedures to ensure that the Company's internal divisions, affiliates, and third parties' use of Demographic Information complies with the Company's use and data limitations.

43. Describe in Detail any methods the Company employs to attempt to determine when a user's account on the Social Media and Video Streaming Service is used by an individual other than the user, Including a malicious attacker, a friend, or a family member.

Children and Teens

44. For each Social Media and Video Streaming Service identified in response to Specification 5:

a) state whether the Company has indicated to any third party or affiliate, Including but not limited to any app store, platform, or advertising network or platform, that the Social Media and Video Streaming Service or portions of content thereof is directed to Children and Teens. If so, Describe in Detail how the Company determines that the Social Media and Video Streaming Service or portions of content thereof are directed to Children and Teens; and

b) Describe in Detail the Company's policies, processes, procedures, and practices regarding users who indicate they are under thirteen years old, and between thirteen and seventeen, inclusively, Including:

i) whether the Company blocks such users from creating an account;

ii) whether the company collects Personal Information of Children or Teens without verified parental consent for "support for internal operations," and if so Describe in Detail all of the internal-operations purposes and the necessity of each piece of Personal Information to accomplish those purposes;

iii) all strategies, plans, presentations, Analyses, machine learning or artificial intelligence, and/or efforts to Identify usage patterns associated with Children and Teens, validate results, and/or monetize this usage, Including all efforts to maintain and/or increase User Engagement by Children and Teens;

iv) each use and its associated value, Including revenue, derived from the Personal Information of Children and Teens collected according to the following categories: (1) with verified consent, (2) without parental consent for "support of internal operations," (3) during usage associated with patterns indicating Children's and Teens' use of an adult account, and (4) without parental consent for another specified reason; and

v) a description of any technical measures to enforce such policies, processes, procedures, and practices.

45. For each Social Media and Video Streaming Service identified in response to Specification 5, Describe in Detail:

a) the intended age range of the user base; and

b) any information in the Company's possession about the actual age of the user base, Including any predictions or calculations of age through machine learning or artificial intelligence.

46. For each Social Media and Video Streaming Service identified in response to Specification 5, Describe in Detail the Company's policies, processes, procedures, and practices when contacted by parents who wish to review or delete Personal Information that has been collected from their Child or Teen, or when the account is otherwise discovered to have been created or posted by a Child or Teen without parental consent.

47. State whether the Company is a member of any self-regulatory organizations or programs Related to children's privacy, Including any FTC-approved Children's Online Privacy Protection Act safe harbor program. If so, Identify each organization and state the dates of membership.

48. For each Social Media and Video Streaming Service identified in response to Specification 5, state whether there are system(s) in place to automatically or algorithmically Identify Children and Teens. If so, Describe in Detail the system(s) in place, Including whether the Company uses any other metrics to determine whether a user is a Child or a Teen.

49. For each Social Media and Video Streaming Service identified in response to Specification 5, Describe in Detail whether the Company has ever relied on verified parental consent provided by an educational institution. To the extent the Company uses the information for commercial purposes, provide the Company's user interfaces for getting consent. Describe in Detail any policies or procedures Relating to the retention or deletion of such data.

Relationship with Other Services

50. Submit all Documents Relating to competition in the sale or provision of each Social Media and Video Streaming Service identified in response to Specification 5, Including, but not limited to, market studies, forecasts, surveys, and all other Documents Relating to:

a) the ability or willingness of customers, consumers, or other Persons to switch to (or from) the Company's products or services from (or to) another product or service, Including by altering relative level of engagement such as time spent;

b) monitoring or collection of information about any other Person's Social Media and Video Streaming Service or Digital Advertising Service;

c) competition to attract, gain, and retain users to, or increase User Engagement with, the Company's Social Media and Video Streaming Services, Including competition to expand or improve product offerings, features, functionality, coverage, user interfaces, product quality, or level of service;

d) the ability or willingness of users to seek access to or use the Company's Social Media and Video Streaming Services while also using Social Media and Video Streaming Services offered by other Persons;

e) competition Relating to data protection and privacy;

f) competition to obtain data, information, or other content for the Company's products or services;

g) the effect of advertising load on (i) consumer or user perceptions or behavior, or (ii) advertising revenue, prices, or profitability;

h) the effect of User Engagement on advertising revenue, prices, or profitability;

i) competition between different types of Digital Advertising Services, or between Digital Advertising Services and any other form of advertising;

j) competition to attract, gain, or retain advertising customers of the Company's Digital Advertising Services, or attempts to win advertising customers or other revenue-generating customers from other companies, and losses of advertising customers or other revenue-generating customers; and

k) the value, Including conversion rate, lead quality, or advertiser return on investment, of the Company's or any other Person's advertising products or services.

51. For each Social Media and Video Streaming Service identified in response to Specification 5, submit all Documents Relating to:

a) barriers to entry into the provision or sale of the Relevant Product, Including but not limited to customer or user lock-in effects, access to user data, and algorithmic sophistication; and

b) switching costs for users, Including loss or lack of access to data specific to any Relevant Product, Including users' social graph and social history, or difficulty in transferring such data.

52. For each Social Media and Video Streaming Service identified in response to Specification 5, Describe in Detail all material changes made by the Company to comply with the European Union's General Data Protection Regulation, Including whether those changes apply exclusively to users in the European Union or also to users in the United States and worldwide. Describe in Detail any material changes to the ability of third parties to access or port data, Including changes to application program interfaces and software development kits.

Other Documents

53. Produce all Documents consulted or otherwise relied on to prepare Your response to this Order that were not otherwise specifically requested.

You are advised that penalties may be imposed under applicable provisions of federal law for failure to file special reports or for filing false reports.

The Special Report called for in this Order is to be filed on or before 45 days from the date of service.

By direction of the Commission, Commissioner Phillips dissenting.

_____

Joseph J. Simons, Chairman

SEAL

December 11, 2020

Attachment A

DEFINITIONS & ADDITIONAL INSTRUCTIONS

A. "**Advertiser Metric**" means, and information shall be provided separately for, each metric of advertising performance or effectiveness that is tracked by, reported on, derived from other data by, or otherwise used by the Company for any Digital Advertising Service.

B. "**Advertising Format**" means, and information shall be provided separately for, each type of ad by media type (e.g., text, photo, or video), ad type (e.g., carousel ad, slideshow ad, collection ad, playable ad), and location (e.g., specific locations on a web page or app) the Company uses to place advertisements for any Person on any Digital Advertising Service or any other application or website, whether or not owned by the Company.

C. "**Advertising Objective**" means, and information shall be provided separately for, each selectable objective offered by the Company to advertisers on any Digital Advertising Service owned by the Company or other platform on which the Company displays advertisements, Including, but not limited to, objectives such as brand awareness, reach, traffic, engagement, app installs, video views, lead generation, messages, conversions, catalog sales, or store traffic.

D. "**Advertising Placement**" means, and information shall be provided separately for, each location where the Company displays advertisements, stated separately for (1) each website, app, or other online platform owned or operated by the Company, and (2) each supply side platform owned or operated by the Company.

E. "**Algorithms or Data Analytics**" means the process of examining and analyzing data in order to find patterns and make conclusions about that data, whether by machine or human analyst.

F. "**Analysis**" or "**Analyses**" Include, but are not limited to, studies, reports, tests, and experiments.

G. The terms "**and**" and "**or**" have both conjunctive and disjunctive meanings as necessary to bring within the scope of this Order anything that might otherwise be outside its scope. The singular form of a noun or pronoun Includes its plural form, and vice versa; and the present tense of any word Includes the past tense, and vice versa.

H. "**Communication**" means any exchange, transfer, or dissemination of information, regardless of the means by which it is accomplished.

I. "**Child**" or "**Children**" means individuals under the age of thirteen (13).

J. "**Classifiers**" means a machine-based process that sorts unlabeled data into categories.

K. "**Company**" means **[COMPANY NAME]**, its domestic and foreign parents, predecessors, divisions, subsidiaries, affiliates, partnerships and joint ventures; and all directors, officers, employees, agents, and representatives of the foregoing. The terms "subsidiary," "affiliate," and "joint venture" refer to any Person in which there is partial (25% or more) or total ownership or control between the Company and any other Person.

L. "**Country Location**" means, and information shall be provided separately for, (1) the United States; (2) Australia; (3) Brazil; (4) Canada; (5) China; (6) France; (7) Germany; (8) India; (9) Indonesia; (10) Italy; (11) Japan; (12) Mexico; (13) the Netherlands; (14) Russia; (15) Saudi Arabia; (16) South Korea; (17) Spain; (18) Switzerland; (19) Turkey; (20) the United Kingdom; and (21) all other countries not in the foregoing list, combined.

M. "**Demographic Information**" means characteristics of human populations, such as age, ethnicity, race, sex, disability, and socio-economic information.

N. "**Describe in Detail**" means providing the information requested in narrative form, Including an explanation of each material change, if any, made during the applicable time period Relating to the practices described, as well as the effective date(s) of the change(s) and the reason(s) for such change(s).

O. "**Digital Advertising Service**" Includes, and information shall be provided separately for: each Company product or offering that serves or displays, or Company service Relating to the service or display of, advertisements through an application or website on any device (e.g., personal computer, iOS device, Android device, etc.).

P. "**Document**" and "**Documents**" mean any information, on paper or in electronic format, Including written, recorded, and graphic materials of every kind, in the possession, custody, or control of the Company. The term "Documents" Includes, without limitation: computer files; email messages; audio files; instant messages; text messages; messages sent on any enterprise messaging system; any other form of electronic message; drafts of Documents; metadata and other bibliographic or historical data describing or Relating to Documents created, revised, or distributed electronically; copies of Documents that are not identical duplicates of the originals in that Person's files; and copies of Documents the originals of which are not in the possession, custody, or control of the Company.

1. Unless otherwise specified, the term "Documents" excludes:

    a. bills of lading, invoices, purchase orders, customs declarations, and other similar Documents of a purely transactional nature;

    b. architectural plans and engineering blueprints;

    c. Documents solely relating to environmental, tax, human resources, OSHA, or ERISA issues; and

    d. relational and enterprise databases, except as required to comply with an individual Specification.

2. The term "computer files" Includes information stored in, or accessible through, computers or other information retrieval systems. Thus, the Company should produce Documents that exist in machine-readable form, Including Documents stored in personal computers, portable computers, workstations, minicomputers, mainframes, servers, backup disks and tapes, archive disks and tapes, and other forms of offline storage, whether on or off Company premises. If the Company believes that the required search of backup disks and tapes and archive disks and tapes can be narrowed in any way that is consistent with the Commission's need for Documents and information, You are encouraged to discuss a possible modification to this Definition with the Commission representative identified on the last page of this Request. The Commission representative will consider modifying this Definition to:

   a. exclude the search and production of files from backup disks and tapes and archive disks and tapes unless it appears that files are missing from those that exist in personal computers, portable computers, workstations, minicomputers, mainframes, and servers searched by the Company;

   b. limit the portion of backup disks and tapes and archive disks and tapes that needs to be searched and produced to certain key individuals, certain time periods, or certain Specifications identified by the Commission representative; or

   c. Include other proposals consistent with Commission policy and the facts of the case.

Q. The terms "**Each**," "**any**," and "**all**" mean "each and every."

R. "**Electronically Stored Information**" or "**ESI**" means the complete original and any non-identical copy (whether different from the original because of notations, different metadata, or otherwise), regardless of origin or location, of any writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any electronic medium from which information can be obtained either directly or, if necessary, after translation by You into a reasonably usable form. This Includes, but is not limited to, electronic mail, instant messaging, videoconferencing, and other electronic correspondence (whether active, archived, or in a deleted items folder), word processing files, spreadsheets, databases, and video and sound recordings, whether stored on: cards, magnetic or electronic tapes, disks, computer hard drives, network shares or servers, or other drives, cloud-based platforms, cell phones, PDAs, computer tablets, or other mobile devices, or other storage media.

S. "**Familial Relationship(s)**" means a description of the Familial Status of all members of a household (e.g., family of four with two parents and two Children).

T. "**Familial Status**" means the familial designation of a natural Person (e.g., spouse, Child, stepchild, parent, grandparent, parent-in-law, sibling-in-law, and child-in-law, among others).

U. "**Identify**" or "**Specify**," when used in reference to a natural Person, mean to state the Person's (1) full name; (2) present or last-known residence and telephone number and present or last-known business address and telephone number; and (3) present or last-known employer and job title. For any Person identified, if any of the above information was different during the time period relevant to the CID, supply both the current information and such different information as applies to the time period relevant to the CID. Once a natural Person has been identified properly, it shall be sufficient thereafter when Identifying that same Person to state the name only.

The terms "Identify" or "Specify," when used in reference to a corporation or other non-natural Person, mean (1) to state that entity's name; (2) to describe its nature (e.g., corporation, partnership, etc.); (3) to state the location of its principal place of business; and (4) to Identify the natural Person or Persons employed by such entity whose actions on behalf of the entity are responsive to the CID. Once such an entity has been identified properly, it shall be sufficient thereafter when Identifying that same entity to state the name only.

The terms "Identify" or "Specify," when used in reference to facts, acts, events, occurrences, Meetings, or Communications, mean to describe, with particularity, the fact, act, event, occurrence, Meeting, or Communication in question, Including, but not limited to, (1) Identifying the participants and witnesses of the fact, act, event, occurrence, Meeting, or Communication; (2) stating the date or dates on which the fact, act, event, occurrence, Meeting, or Communication took place; (3) stating the location(s) at which the fact, act, event, occurrence, Meeting, or Communication took place; and (4) providing a description of the substance of the fact, act, event, occurrence, Meeting, or Communication.

V. The terms "**Include**" and "**Including**" mean "including, but not limited to." The use of the term "Include" in any request shall not be used to limit the generality or scope of any request. Nor shall the generality of any request be limited by the fact that another request touches on the same topic with a greater or lesser degree of specificity.

W. "**Meeting**" means an assembly of two or more people, in-person or via telephone, voice-over-IP, video, video conferencing, WebEx, chat messaging, or similar means of Communication.

X. "**Order**" means the Order, Including the attached Resolution, Specifications, and Attachment.

Y. "**Person**" Includes the Company and means any natural person, corporate entity, partnership, association, joint venture, government entity, or trust.

Z. "**Personal Information**" means information about a specific individual or Device, Including: (1) first and last name; (2) home or other physical address, Including street name and name of city or town, or other information about the location of the individual, Including but not limited to location from cellular tower information, fine or coarse location, or GPS coordinates; (3) Email address or other online contact information, such

as an instant Messaging user identifier or screen name; (4) telephone number; (5) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a device identifier, a device fingerprint, a hashed identifier, or a processor serial number; (6) nonpublic Communications and content, Including, but not limited to, e-mail, text messages, contacts, photos, videos, audio, or other digital images or audio content; (7) Internet browsing history, search history, or list of URLs visited; (8) video, audio, cable, or TV viewing history; (9) biometric data; (10) health or medical information; (11) Demographic Information or (12) any other information associated with that User or Device.

AA. "**Publisher**" means any Person paid to show an advertisement to consumers.

BB. "**Relate**," "**Related to**," and "**Relating to**" mean, in whole or in part, addressing, analyzing, concerning, constituting, containing, commenting on, discussing, describing, Identifying, referring to, reflecting, reporting on, stating, or dealing with.

CC. "**Relevant Area**" means, and information shall be provided separately for, (1) the United States, and (2) worldwide.

DD. "**Relevant Product**" Includes, and information shall be provided separately for, any Social Media and Video Streaming Service or Digital Advertising Service.

EE. "**Selected Advertiser Attribute**" means, and information shall be provided separately for, (1) the five (5) Advertiser Attributes that the Company uses most frequently in the provision or sale of advertising, and (2) each of the following Advertiser Attributes:

a. industry vertical (e.g., ecommerce, consumer packaged goods, professional services);

b. advertiser size (e.g., global business group, small business group);

c. advertising spend tier or bracket; and

d. status (e.g., active, inactive).

FF. "**Selected Advertiser Category**" means, and information shall be provided separately for, each mutually exclusive group of advertisers resulting from every combination of values across each Selected Advertiser Attribute.

For illustration purposes, assume "advertiser size," "industry vertical," and "spend tier," are the Selected Advertiser Attributes. Assume further that "small business," and "large business" are mutually exclusive values for the "advertiser size" attribute; "ecommerce" and "gaming" are mutually exclusive values for the "industry vertical" attribute; and "1" and "2" are mutually exclusive values for the "spend tier" attribute. In this example, "ecommerce small business with spend tier 1" and "ecommerce small business with spend tier 2" are mutually exclusive Selected Advertiser Categories.

GG. "**Selected User Attribute**" means, and information shall be provided separately for, each of the following User Attributes: (1) age; (2) gender; (3) Country Location of the user; (4) network size; (5) education; (6) income; (7) race and ethnicity; (8) registration status of the user (e.g., registered or non-registered).

HH. "**Selected User Group**" means, and information shall be provided separately for, each mutually exclusive group of users reflecting each mutually exclusive combination of values from the Selected User Attributes.

II. "**Social Media and Video Streaming Service**" Includes, and information shall be provided separately for, any product or service that allows users to create and share content with other users (whether a private or group interaction) through an application or website on any device (e.g., personal computer, iOS device, Android device, etc.), or stream video, Including, but not limited to, any social networking service, messaging service, video streaming service, or photo, video, or other content sharing application, whether offered for a fee or for free.

JJ. "**Teen**" or "**Teens**" means individuals between the ages of thirteen (13) and seventeen (17), inclusively.

KK. "**Third-Party Category**" means, and information shall be provided separately for, each type of Person (e.g., app developers, analytic partners, or advertisers) with whom the Company provides application programming interface ("API") access or shares data, or with whom the Company otherwise has a business relationship.

LL. "**User Attribute**" means, and information shall be provided separately for, each attribute or categorization of any user (e.g., age, gender, country, language, categorizations based on user interests, or categorizations based on other user behavior) of any Social Media and Video Streaming Service that is tracked or used by the Company for any purpose, Including, but not limited to, the provision or sale of any Social Media and Video Streaming Service or advertising.

MM. "**User Engagement**" means how a user, on and off the Social Media and Video Streaming Service, interacts with any product or service of the Social Media and Video Streaming Service (Including, but not limited to, how frequently, for how long, and in what manner).

NN. "**User Metric**" means, and information shall be provided separately for, each metric for user interaction with any web site or application owned or operated by any Person (Including the Company) on any device (e.g., personal computer, iOS device, or Android device).

OO. "**User Network Size**" means, and information shall be provided separately for, each metric for the size of a user's network within any Social Media and Video Streaming Service owned by any Person (Including the Company), Including, but not limited to, the number of a user's friends, the number of a user's followers, the number of other users that a user follows, the number of a user's reciprocal followers, and the number of telephone contacts stored by a user.

PP. "**You**" and "**Your**" means the individual or entity to whom this Order is issued and Includes the "Company."

QQ. **Meet and Confer**: You are encouraged to contact **Andrea Arias** at **(202) 326-2715** or **Caroline Schmitz** at **(202) 326-2621** as soon as possible to schedule a Meeting (telephonic or in person) in order to confer regarding Your response.

RR. **Modification of Specifications**: If You believe that the scope of the required search or response for any specification can be narrowed consistent with the Commission's need for Documents or information, You are encouraged to discuss such possible modifications, Including any modifications of definitions and instructions, with the Commission counsel named above.

SS. **Electronic Submission of Documents**: See the attached "Federal Trade Commission, Bureau of Consumer Protection Production Requirements," which details all requirements for submission of information, generally requiring that files be produced in native form and Specifying the metadata to be produced. As noted in the attachment, some items require discussion with the FTC counsel **prior to** production, which can be part of the general "Meet and Confer" described above. If You would like to arrange a separate discussion involving Persons specifically familiar with Your ESI systems and methods of retrieval, make those arrangements with FTC counsel when scheduling the general meet and confer discussion.

TT. **Applicable Time Period**: Unless otherwise directed in the Specifications, the applicable time period for the request shall be from **January 1, 2019 until the date of full and complete compliance with this Order**.

UU. **Document Production**: Because postal delivery to the Commission is subject to delay due to heightened security precautions, please use a courier service such as Federal Express or UPS.

VV. **Production of Copies**: Copies of marketing materials and advertisements shall be produced in color, and copies of other materials shall be produced in color if necessary to interpret them or render them intelligible.

WW. **Sensitive Personally Identifiable Information**: If any material called for by these requests contains sensitive Personally Identifiable information or sensitive health information of any individual, please contact us before sending those materials to discuss ways to protect such information during production. For purposes of these requests, sensitive Personally Identifiable information Includes: an individual's Social Security number alone; or an individual's name or address or telephone number in combination with one or more of the following: date of birth, Social Security number, driver's license number or other state identification number, or a foreign country equivalent, passport number, financial account number, credit card number, or debit card number. Sensitive health information Includes medical records and other individually identifiable health information Relating to the past, present, or future physical or mental health or conditions

of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

APPENDIX A

The Selected User Attributes (including the values associated with each Selected User Attribute) and User Metrics identified in this Appendix are exemplary, and are not intended to limit the Company's response to the CID.

Selected User Attribute Definitions

Age	Origin	Country
1 (0-25)	Yes	US
2 (26-50)	No	Other
3 (50+)	Missing	Missing
4 (Missing)		

Example Data

Selected User Attributes				Period		User Metrics				
Age	Origin	Country	Number of Registered Users	Month	Year	Number of MAUs	Average Time Spent per MAU	Total Time Spent (Hours)	Average Posts per MAU	Total Posts
1	Yes	US	13	Jan	2010	10	2.7	27	2.0	20
2	Yes	US	15	Jan	2010	12	2.8	33	2.3	27
3	Yes	US	16	Jan	2010	13	3.7	48	2.5	32
4	Yes	US	6	Jan	2010	3	2.7	8	2.3	7
1	No	US	11	Jan	2010	8	2.6	21	4.4	35
2	No	US	12	Jan	2010	9	2.7	24	6.2	56
3	No	US	13	Jan	2010	10	4.5	45	4.0	40
4	No	US	5	Jan	2010	2	3.0	6	7.0	14
1	Missing	US	5	Jan	2010	2	2.5	5	3.0	6
2	Missing	US	5	Jan	2010	2	3.0	6	4.0	8
3	Missing	US	5	Jan	2010	2	4.5	9	3.5	7
4	Missing	US	4	Jan	2010	1	1.0	1	2.0	2
1	Yes	Other	14	Jan	2010	11	7.3	80	2.7	30
2	Yes	Other	18	Jan	2010	15	2.8	42	4.7	70
3	Yes	Other	17	Jan	2010	14	5.6	78	6.5	91
4	Yes	Other	7	Jan	2010	4	2.8	11	4.5	18
1	No	Other	23	Jan	2010	20	2.9	57	4.8	95
2	No	Other	8	Jan	2010	5	2.4	12	3.2	16
3	No	Other	9	Jan	2010	6	2.5	15	2.5	15
4	No	Other	4	Jan	2010	1	3.0	3	4.0	4
1	Missing	Other	6	Jan	2010	3	4.7	14	4.3	13
2	Missing	Other	5	Jan	2010	2	2.5	5	4.5	9
3	Missing	Other	5	Jan	2010	2	4.5	9	5.5	11
4	Missing	Other	4	Jan	2010	1	1.0	1	2.0	2
1	Yes	Missing	10	Jan	2010	7	9.6	67	4.3	30
2	Yes	Missing	18	Jan	2010	15	2.8	42	4.7	70
3	Yes	Missing	15	Jan	2010	12	6.4	77	8.1	97
4	Yes	Missing	9	Jan	2010	6	2.2	13	3.8	23
1	No	Missing	21	Jan	2010	18	3.3	59	4.9	89
2	No	Missing	10	Jan	2010	7	1.7	12	2.3	16
3	No	Missing	8	Jan	2010	5	2.6	13	3.8	19
4	No	Missing	5	Jan	2010	2	1.5	3	2.0	4
1	Missing	Missing	7	Jan	2010	4	3.5	14	2.0	8
2	Missing	Missing	8	Jan	2010	5	1.0	5	1.4	7
3	Missing	Missing	5	Jan	2010	2	4.5	9	6.5	13
4	Missing	Missing	5	Jan	2010	2	3.0	6	3.5	7

APPENDIX B

The Selected Advertiser Attributes (including the values associated with each Selected Advertiser Attribute) and Advertiser Metrics identified in this Appendix are exemplary, and are not intended to limit the Company's response to the CID.

Selected Advertiser Attribute Definitions

Advertiser Size	Industry Vertical	Spend Tier
1 (Small business)	Ecommerce	1
2 (Large business)	Gaming	2
3 (Missing)	Missing	

Example Data

Selected Advertiser Attributes			Period		Advertiser Metrics			
Advertiser Size	Industry Vertical	Spend Tier	Month	Year	Number of Advertisers	Total Ad Revenue	Total Number of Auctions	Average Winning Advertiser Bid
1	Ecommerce	1	Jan	2010	10	$ 90,000	27	$ 16.50
2	Ecommerce	1	Jan	2010	12	$ 110,000	33	$ 8.50
3	Ecommerce	1	Jan	2010	13	$ 110,000	33	$ 6.55
1	Gaming	1	Jan	2010	8	$ 70,000	21	$ 1.76
2	Gaming	1	Jan	2010	9	$ 80,000	24	$ 8.15
3	Gaming	1	Jan	2010	10	$ 90,000	27	$ 2.35
1	Missing	1	Jan	2010	7	$ 60,000	23	$ 2.67
2	Missing	1	Jan	2010	5	$ 55,000	17	$ 5.13
3	Missing	1	Jan	2010	4	$ 50,000	12	$ 9.15
1	Ecommerce	2	Jan	2010	11	$ 100,000	30	$ 3.35
2	Ecommerce	2	Jan	2010	15	$ 130,000	39	$ 7.15
3	Ecommerce	2	Jan	2010	14	$ 130,000	39	$ 1.45
1	Gaming	2	Jan	2010	20	$ 190,000	57	$ 3.07
2	Gaming	2	Jan	2010	5	$ 40,000	12	$ 25.10
3	Gaming	2	Jan	2010	6	$ 40,000	12	$ 30.25
1	Missing	2	Jan	2010	9	$ 80,000	21	$ 15.80
2	Missing	2	Jan	2010	7	$ 65,000	13	$ 12.30
3	Missing	2	Jan	2010	3	$ 25,000	8	$ 13.50

Federal Trade Commission

ftc.gov