Hal J. Singer
Managing Director of Econ One, Adjunct Professor of the University of
Utah, and Executive Director of the Utah Project

Augustus H. Urschel
Economist of Econ One

Comments in Response to the Federal Trade Commission's Advance
Notice of Proposed Rulemaking for a Trade Regulation Rule on
Commercial Surveillance and Data Security
"Commercial Surveillance ANPR, R111004"

Commercial Surveillance ANPR, R111004

Comments of Hal J. Singer and Augustus H. Urschel[1]

Executive Summary

We have been asked by the News Media Alliance[2] to respond to questions posed by the Federal Trade Commission (FTC) in their Advance Notice of Proposed Rulemaking (ANPR) regarding commercial surveillance and data security.[3] We respond to questions 39, 41, and 43-47.

To track the definitions used in the ANPR, in this comment we refer to users and consumers (whether they are individuals, workers, or businesses) of internet-based products and services as "consumers," and the providers of those internet-based products and services (collectively, "digital properties") as "companies."[4] We refer to Alphabet (Google), Meta (Facebook), and their subsidiaries as the "dominant tech platforms." We use the term "publisher" to refer to any other company that collects consumer data and sells "inventory," or ad space, to advertisers.[5] Finally, rather than use the broader term of "commercial surveillance," our comment specifically focuses on the practice of what we call "data poaching."[6] "Data poaching" is when *a third-party entity* collects consumer data via the use of an embedded piece of code on a publisher's digital property. This contrasts with traditional "data collection," which occurs when a publisher collects data on its own consumers using its own digital properties. We use the term "embeds" to refer to code, packages, plug-ins, integrations, iframes, or software tools developed by a third-party that provide some service to a publisher.

We find that Alphabet and Meta have used their market power in the markets of search and social media, respectively, and the associated digital advertising market to collect consumer data throughout the internet, exceeding the narrow bounds of the quid pro quo "service for data" arrangements that consumers expect. The dominant tech platforms have turned their digital advertising *rivals* into *resources* by siphoning first-party consumer data generated by publishers on their own digital properties through the use of embeds. By poaching this data and using it in a way not directed by the publisher that owns or operates the underling digital property, Alphabet and Meta have eroded the competitive value of their rival's first-party consumer data in

---

digital advertising market. This ability to collect consumer data *even when consumers are engaged in activity away from the dominant tech platform's branded properties* allows each platform to "fully track" a single consumer throughout the internet. This had lead to an erosion of consumer trust, clouds consumer expectations about who collects and uses their data, and weakens competition in the market for digital advertising.

We propose a data poaching rule that would prevent the dominant tech platforms from collecting consumer data from independent digital properties via embeds. The rule *would grant the company with which the consumer interacts the exclusive right to all first-party consumer data created*—that is, this rule would ensure that the quid pro quo of "service for data" is between the consumer and the company with which they interact, creating a clear consumer expectation of who collects their data. Under the data poaching rule, third parties could still temporarily collect and process consumer data in accordance with the service they provide the rights holder, but they could not retain this data for other commercial purposes. The rule would prohibit Alphabet and Meta from automatically collecting user data from publisher websites, apps, and other digital services through embeds such as AdSense, Admob, Meta Pixel, and Meta partnership programs.

The dominant tech platforms would bear the cost of such a rule, benefitting both consumers and publishers in digital advertising market. We estimate that the cost of the data poaching rule to Alphabet and Meta would be approximately ten percent of their digital current advertising revenues, which would result in a concomitant increase in digital advertising revenues for independent publishers. Consumers would benefit directly through a more transparent consumer standard on data collection and through lessened exposure from data breaches. Consumers would also benefit indirectly through the lowering of online subscription prices, as implied by a two-sided pricing model. Finally, consumers would also indirectly benefit from the reinvestment of these shifted advertising revenues into the digital content they consume generally—and journalism specifically with its attendant social benefits.

Question 39: The FTC Should Enact A "Data Poaching" Rule That Prevents the Dominant Tech Platforms from Collecting Data via Embeds

Question 39 asks: "To what extent, if at all, should the Commission limit companies that provide any specifically enumerated services (e.g., finance, healthcare, search, or social media) from owning or operating a business that engages in any specific commercial surveillance practices like personalized or targeted advertising? If so, how? What would the relative costs and benefits of such a rule be, given that consumers generally pay zero dollars for services that are financed through advertising?"

Answer: The Commission should enact a data poaching rule that would grant the sole right to collect consumer data to the known owner or operator of the digital property with whom the consumer interacts. A data poaching rule would both benefit consumers directly via a clear consumer expectation standard, and indirectly through a host of positive downstream effects caused by increased competition in the digital advertising market. This could also lead to lower prices paid by consumers. The costs of this rule would be borne solely by the dominant tech platforms that surreptitiously and persistently track consumers. We explain these findings in detail below.

A.   **The Dominant Tech Platforms Use Their Market Power to Poach Consumer Data from Third Parties**

1.   **The Economic "Quid Pro Quo" Between Consumers and Online Companies: Data for Service**

The prevailing business model for companies providing free services over the internet—such as entertainment, informational content, search, or social media—is based on the monetization of consumer data. Consumers of free online services enter an implicit and narrow quid pro quo: In exchange for forgoing monetary payment in part or in whole for use of a digital property, consumers allow online companies to collect their data while using the digital property.

Consumer data are monetized through digital advertising, estimated to be a $150 to $210 billion industry in the United States in 2021.[7] Three players dominate the industry: Alphabet (29 percent of U.S. digital advertising revenue), Meta (24

---

[7] Estimates include $153.2 billion, $189.3 billion, and $211.20 billion in 2021. *See respectively IAB and PwC, Outlook 2022: The US Digital Advertising Ecosystem*, IAB (Oct. 2021), at 4, *available at* https://www.iab.com/wp-content/uploads/2021/10/IAB-PWC-Outlook-2022-The-Digital-Advg-Ecosystem-Oct-2021.pdf; *Internet Advertising Revenue Report*, INTERACTIVE ADVERTISING BUREAU (Apr. 2022), at 6, *available at* https://www.iab.com/wp-content/uploads/2022/04/IAB_Internet_Advertising_Revenue_Report_Full_Year_2021.pdf; Sarah Lebow, *Google, Facebook, and Amazon to account for 64% of US digital ad spending this year*, INSIDER INTELLIGENCE (Nov. 3, 2021), *available at* https://www.insiderintelligence.com/content/google-facebook-amazon-account-over-70-of-us-digital-ad-spending.

percent), and Amazon (12 percent).[8] Digital advertising is segmented by the format in which it is presented to the consumer. In 2021, 41 percent of all digital advertising dollars went to search advertisements (linking an advertisement to a search word or phrase), 30 percent went to display ads (ad banners on websites), and 21 percent went to video ads (advertising that appears before, during, or after digital video content).[9]

Data collected by a firm about its own consumers is known as "first-party data."[10] Consumer data used by other firms who do not have a direct relationship with the consumer are known as "third-party data."[11] First-party data are, in theory, proprietary to the company that collects it. Third-party data are data purchased by publishers from data aggregators to augment their first-party data.

When a publisher seeks to place advertisements, it sorts consumers who frequently traffic its digital property into groups based on their data. The publisher then markets these consumers using their digital property (advertising inventory) to advertisers seeking to display ads to reach relevant consumers.

In the online advertising market, consumers for a publisher has rich first-party data represent the "premium inventory." Rich first-party data permit precise targeting of advertisements. Consumers with little or no rich first-party data associated with them, or who are in otherwise undesirable advertising demographics, are less valuable inventory. Premium inventory is usually sold manually (that is, the sale occurs between two negotiating humans), while the ads shown to less desirable consumers are typically sold through automated auctions run by third-party advertising exchanges.

Companies that collect first-party data compete in the digital advertising market for finite (but growing year over year) advertising budgets, resulting in an arms race for richer, more predictive first-party consumer data. Richer data yields better targeting, which yields a higher clickthrough rate, which yields a more efficient use of advertising dollars, which in turn attracts more advertising dollars to sellers who collect the most data.

---

[8] Sarah Lebow, *Google, Facebook, and Amazon to account for 64% of US digital ad spending this year*, INSIDER INTELLIGENCE (Nov. 3, 2021), *available at* https://www.insiderintelligence.com/content/google-facebook-amazon-account-over-70-of-us-digital-ad-spending.

[9] Eight percent went to other advertising formats. *Id.* at 17.

[10] *Investigation of Competition in Digital Markets*, *Majority Staff Report and Recommendations*, SUBCOMMITTEE ON ANTITRUST, COMMERCIAL AND ADMINISTRATIVE LAW OF THE COMMITTEE ON THE JUDICIARY (Oct. 2020), at 129 [hereafter Majority Report], *available at* https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf. *See also Competition and data protection in digital markets,* COMPETITION & MARKETS AUTHORITY (May 19, 2021), at 11*, available at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf.

[11] *Id.*

2. The Dominant Tech Platforms Collect Data from Consumers' Use of Other Companies' Digital Properties

Alphabet and Meta own multiple digital properties that individually generate vast amounts of valuable first-party data for advertisers. Alphabet's main properties in the publishing space are Google Search, Android, Chrome, and Gmail. Meta's main properties in this space are Facebook, Instagram, and WhatsApp. In exchange for use of these services, Alphabet and Meta offer the standard quid pro quo to consumers: free service for data, which is then used to sell targeted advertising. In this sense, the dominant tech platforms are little different from other internet companies they compete with for digital advertising dollars.

But the similarities end there, because the dominant tech platforms *also* collect consumer data from *independent publisher websites and apps.* Using their market power in the related markets of social media, search, and ad tech, Alphabet and Meta have transformed their ubiquitously employed embeds into listening devices, which turns independent publishers—Alphabet and Meta's *competitors in digital advertising market*—into data collection resources. This allows Alphabet and Meta to poach the *same first-party data collected by the publisher*.[12] In other words, the dominant tech platforms use their platform power to turn their *rivals* into *resources* in the digital advertising market, degrading the value of their competitors' data in the process.

The technical mechanisms that allow data poaching are complex and varied. Broadly speaking, embeds include plugins on websites, cookies, browser add-ons, mobile app support, and tools that allow a third-party website to analyze its own user traffic. They also include integrations with Alphabet or Meta services such as Maps, the "Like" button, and integration with YouTube or Facebook comments.[13] Even the

---

[12] *See, e.g.,* Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance In Spite Of Consumers' Preference For Privacy*, 16(1) BERKELEY BUSINESS LAW JOURNAL 39–101, 72 (2019) [hereafter Case Against Facebook] ("Now Facebook would receive the ability to monitor the behavior of their customers—competitors with Facebook in the digital advertising market—by changing the fine print of permissions. Facebook increasingly knew as much about The Wall Street Journal's readers as the Journal did itself. Furthermore, unlike the Journal, Facebook now knew which Journal readers were avid ESPN readers, giving it the capability to bundle and sell targeted audiences, which further commoditized the value of competitors' inventory. Under the new regime, when a consumer visited a website with a Facebook plugin, Facebook piggybacked onto the requests and responses necessary to simply display the plugins, to now also surveil the users of competitor ad sellers—rendering the Facebook code a Trojan Horse of sorts.").

[13] *See Social Plugins*, FACEBOOK, META FOR DEVELOPERS, *available at* https://developers.facebook.com/docs/plugins; GOOGLE, *The Maps Embed API overview, available at* https://developers.google.com/maps/documentation/embed/get-started; *Embed videos & playlists*, GOOGLE, *available at* https://support.google.com/youtube/answer/171780?hl=en; *Single sign-on (SSO) embedding*, GOOGLE, *available at* https://cloud.google.com/looker/docs/single-sign-on-embedding; *Connect to AdSense and show ads on your WordPress site*, GOOGLE, *available at* https://support.google.com/adsense/answer/7527509?hl=en. *See also* Dave Davies, *How Tech Companies Track Your Every Move and Put Your Data Up For Sale*, NPR (Jul, 31, 2019), *available at*

fundamental tools for monetizing a website allow data poaching. For example, Alphabet's advertising tools such as Adsense and Admob allow Alphabet to passively collect consumer data such as GPS location, age, and gender when a consumer uses any digital property that has one of these embeds installed.[14] Meta similarly tracks consumer activity through a suite of embeds.[15] Meta also operates the "Meta Pixel," which tracks internet users across more than six million websites regardless of whether they have an account with Meta services.[16] *Any website* with a Facebook button on it is tracking users whether or not they have a Facebook account.[17] Moreover, Alphabet and Meta (along with other companies such as Apple) also offer a Single Sign-On feature to allow users to log on to third-party websites using an existing platform account.[18] While convenient for consumers, these Single Sign-On features can also give the dominant tech platforms another way to poach first-party data generated on the independent digital property.[19]

Suppose a hypothetical website features articles and review aobut electric bicycles ("e-bikes"). After achieving some initial success, the website wishes to monetize the site by displaying banner ads to its to visitors, who presumably have an interest in e-bikes, a valuable piece of first-party data. If the website integrates Google AdSense to sell ads, it would accomplish this goal and could sell e-bike related banner ads. But in the process of serving ads to its users, Alphabet records who visits the site and is able to match their "e-bike interest" with their *preexisting user data from other sites*. Further, it is able to track information on what ad was served, how or if a consumer interacted with the ad, and places a cookie on the consumer's device in case

https://www.npr.org/2019/07/31/746878763/how-tech-companies-track-your-every-move-and-put-your-data-up-for-sale.

[14] Douglas C. Schmidt, *Google Data Collection*, INSTITUTE FOR SOFTWARE-INTEGRATED SYSTEMS, VANDERBILT UNIVERSITY (Aug. 15, 2018) [hereafter *Google Data Collection*] at 18-19, *available at* http://www.dre.vanderbilt.edu/~schmidt/PDF/google-data-collection.pdf.

[15] Andreea M. Belu, *The Massive Data Collection by Facebook – Visualized,* DATA ETHICS (Jun. 6, 2017), *available at* https://dataethics.eu/facebooks-data-collection-sharelab/.

[16] *Websites using Facebook Pixel*, BUILTWITH (Sept. 23, 2022), *available at* https://trends.builtwith.com/websitelist/Facebook-Pixel#:~:text=Facebook%20Pixel%20is%20a%20mega,see%20our%20Mega%20Technology%20Datasets. *See also* Natasha Singer, *What You Don't Know About How Facebook Uses Your Data,* NEW YORK TIMES (Apr. 11, 2018), *available at* https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html.

[17] Alex Kantrowitz, *Here's How Facebook Tracks You When You're Not On Facebook*, BUZZFEED NEWS (Apr. 11, 2018), *available at* https://www.buzzfeednews.com/article/alexkantrowitz/heres-how-facebook-tracks-you-when-youre-not-on-facebook.

[18] *Single Sign-On,* GOOGLE, *available at* https://cloud.google.com/architecture/identity/single-sign-on; *Facebook Login,* FACEBOOK, META FOR DEVELOPERS, *available at* https://developers.facebook.com/docs/facebook-login/; *Intro to Single sign-on with Apple devices*, APPLE, *available at* https://support.apple.com/guide/deployment/intro-to-single-sign-on-depfdbf18f55/web.

[19] Jefferson Graham, *Is Facebook listening to me? Why those ads appear after you talk about things*, USA TODAY (Jun. 27, 2019), *available at* https://www.usatoday.com/story/tech/talkingtech/2019/06/27/does-facebook-listen-to-your-conversations/1478468001/.

they later purchase the advertised product in a different session.[20] This means that Alphabet can now identify a user as having an e-bike interest *even when they leave the site.* Meaning, even though this hypothetical website generated the first party datapoint of e-bike interest, Alphabet copies that information and retains it in its (far more complete) database on that particular user after they have left the website.[21] The value of the first-party data, earned through the effort the website put into creating its e-bike content, has been effectively stolen by Alphabet. If an e-bike manufacturer wished to display ads for a new e-bike model, it would likely spend its advertising dollars on Google Search banner ads (which uses datapoints from a user's entire internet history) instead of the e-bike website (which uses a single datapoint).

These embeds, which were initially offered as useful tools to publishers, became data poaching devices for the dominant tech platforms after they achieved widespread use. For example, in 2014, Facebook changed its terms of service overnight to allow its embeds to begin tracking consumers across the internet.[22] These embeds also have an extraordinary reach: In 2018, more than one million mobile apps used AdMob, 15 million websites used Adsense, and 30 million websites used Google Analytics.[23] Privacy researchers have discovered that Alphabet has the ability to link this "passively collected" data with a consumer's personal information from other Alphabet services and products.[24]

As a result, it is functionally impossible for consumers to not have their personal data collected by Alphabet or Meta, even if they explicitly try to avoid Alphabet's and Meta's flagship digital properties.

The scope of these extraordinary data collection networks allows Alphabet and Meta to create hyper-specific profiles of each consumer. The data from individual products and services taken alone, such as search history or location data, are extremely valuable. Much like the pieces of a jigsaw puzzle combine to offer a clear image, the combination of these individual sources of consumer data throughout the internet create a picture of each consumer that the firms can use to make *predictive analyses of individuals' behavior.*[25] These data can also be exploited for political purposes, as seen in the 2016 Cambridge Analytica scandal, which revealed that a UK

---

[20] *Google Data Collection* at 18.

[21] Researchers determined that Google is able to easily de-anonymize and match consumer data. *Google Data Collection* at 19–22.

[22] Case Against Facebook, at 70, *citing Making Ads Better and Giving People More Control Over the Ads They See*, FACEBOOK (June 12, 2014), *available at* https://about.fb.com/news/2014/06/making-ads-better-and-giving-people-more-control-over-the-ads-they-see/.

[23] *Google Data Collection* at 15.

[24] *Id.* at 19—22.

[25] Sam Biddle, *Facebook Uses Artificial Intelligence to Predict Your Future Actions for Advertisers, Says Confidential Document*, THE INTERCEPT (Apr. 13, 2018), *available at* https://theintercept.com/2018/04/13/facebook-advertising-data-artificial-intelligence-ai/; *Predictive audiences*, GOOGLE, *available at* https://support.google.com/analytics/answer/9805833?hl=en.

consulting firm used Facebook's consumer data to influence the 2016 U.S. election.[26]

3. The Dominant Tech Platforms' Unfettered Market Power in Related Industries Has Enabled this Widespread Surveillance

Alphabet and Meta use their market power in related markets to dominate the digital marketing industry. In 2021, Alphabet and Meta accounted for 64 percent of digital advertising spending in the United States.[27] Alphabet alone accounted for a 58 percent share of all search advertising revenue in the United States.[28]

High market shares in related industries fuel such digital advertising dominance, giving each firm the ability to turn their embeds in those related markets into consumer data resources. As of July 2020, Alphabet accounted for a 89 percent of all U.S. internet searches.[29] Alphabet also dominates the very devices used to engage with the internet. Google Chrome is the most popular desktop internet browser in the United States with a 61 percent market share,[30] while the Android operating system holds a 46 percent market share in the United States (compared to 70 percent globally).[31] Similarly, Meta (including its acquisitions of Instagram and WhatsApp) is by far the most popular social networking platform on the planet. As of December 2019, Facebook had 1.8 billion monthly active persons (MAP), WhatsApp

---

[26] Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, NEW YORK TIMES (Apr. 4, 2018), *available at*
https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[27] Sara Lebow, *Google, Facebook, and Amazon to account for 64% of US digital ad spending this year*, INSIDER INTELLIGENCE (Nov. 3, 2021), *available at*
https://www.insiderintelligence.com/content/google-facebook-amazon-account-over-70-of-us-digital-ad-spending.

[28] For example, Google accounts for a 58 share of all search advertising revenue in the United States. *Google Collects More Than Half of All US Search Ad Revenue,* INSIDER INTELLIGENCE, *available at* https://www.insiderintelligence.com/content/google-collects-more-than-half-of-all-us-search-ad-revenue.

[29] Composed of U.S. desktop search (81 percent) and mobile search (94 percent) markets. *Id.* at 78 (citing *Desktop & Mobile Search Engine Market Share United States Of America, January 2009 to September 2020*, STATCOUNTER, *available at* https://gs.statcounter.com/search-engine-market-share/desktop-mobile/unitedstates-of-america/#monthly-200901-202009). Note, The Apple iPhone's Safari browser runs through Google. Kate O'Flaherty, *Apple And Google's Secretive iPhone Deal Suddenly Exposed*, FORBES (Sept. 4, 2021), *available at*
https://www.forbes.com/sites/kateoflahertyuk/2021/09/04/apple-google-search-deal-impacts-millions-of-iphones/?sh=5e89ed996483.

[30] Lionel Sujay Vailshery, *U.S. desktop internet browsers market share 2015-2022*, STATISTA (Aug. 5, 2022), *available at* https://www.statista.com/statistics/272697/market-share-desktop-internet-browser-usa/; Kate O'Flaherty, *It's time to ditch Chrome*, WIRED (Jun. 6, 2021), *available at* https://www.wired.co.uk/article/google-chrome-browser-data.

[31] *Share of mobile operating systems in North America 2018-2021, by month*, STATISTA (May 23, 2022), *available at* https://www.statista.com/statistics/1045192/share-of-mobile-operating-systems-in-north-america-by-month/. Federica Laricchia, *Market share of mobile operating systems worldwide 2012-2022*, STATISTA (Aug. 30, 2022), *available at*
https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/.

had 2.0 billion MAP, and Instagram had 1.4 billion MAP. [32] Its closest social networking competitors had far fewer monthly active users: Snapchat had 443 million MAP, Twitter had 582 million MAP, and LinkedIn had 260 million MAP.[33] Meta reports 2.5 billion daily active users across its family of social networking platforms.[34] From September 2017 to September 2018, Facebook alone reached more than 75 percent of U.S. internet users.[35]

These high market shares, combined with significant entry barriers, reflect real market power.[36] The U.S. House Subcommittee on Antitrust, Commercial and Administrative Law concluded in October 2020 that "Google and Facebook both have a significant lead in the market [for digital advertising] due to their significant collection of behavioral data online, which can be used in targeted advertising."[37] In related markets for user data collection, the subcommittee found that "Google has a monopoly in the markets for general online search and search advertising,"[38] and that Facebook "has monopoly power in the market for social networking."[39]

4.   Consumers Are Materially Harmed and Feel Exploited

Alphabet's and Meta's data poaching harms consumers in two ways: Materially, though reducing competition for digital advertising dollars, and psychologically, through their opaque and ominous surveillance practices.

---

[32] Majority Report at 132.

[33] *Id*. at 92. The House Report does not consider TikTok to be a social media platform. *Id*. at 93 ("Although it meets the broad definition of social media as a social app for distributing and consuming video content, TikTok is not a social network."). LinkedIn has been relegated to a "niche strategy" of appealing to professional connections. *Id*. at 91. It bears noting that the FTC's recent antitrust complaint against Facebook does not include LinkedIn in the relevant market definition. Complaint, Federal Trade Commission v. Facebook Inc., Dec. 9, 2020 [hereafter Facebook Complaint], at 58. ("Personal social networking is distinct from, and not reasonably interchangeable with, specialized social networking services like those that focus on professional connections."). We nonetheless reference LinkedIn's statistics here to be over-inclusive.

[34] *Id*. at 132.

[35] *Id*. at 137 (citing FB-HJC-ACAL-00111406 (Oct. 2018) [hereafter Cunningham Memo]).

[36] Combined shares greater than 50 percent are consistent with collective market power under U.S. antitrust jurisprudence. The concept of collective market power is well-understood in antitrust. *See, e.g*., Remarks of J. Thomas Rosch Commissioner, Federal Trade Commission, June 1, 2009 ("But firms who are participants in a duopoly or a tight oligopoly market collectively enjoy power that is akin to monopoly power in the sense that they have the power to increase prices and reduce output in the market as a whole."); Daniel Crane, *Market Power Without Market Definition*, 90 (1) NOTRE DAME LAW REV. 31-79, (2014) ("The Justice Department's high-profile case against Apple and five major book publishers concerning e-book pricing rests on seemingly obvious evidence of the exercise of collective market power creating anticompetitive effects."); Einer Elhauge, *How Horizontal Shareholding Harms Our Economy—And Why Antitrust Law Can Fix It*, HARVARD BUS. LAW. REVIEW 207-286, (2020) ("To whatever extent one thinks managers do pay attention to vote share or re-election odds, this new economic analysis mathematically proves that prices will be increased by high levels of horizontal shareholding across a set of firms that have collective market power.").

[37] Majority Report at 131.

[38] *Id.* at 14.

[39] *Id.* at 12.

First, the ability of Alphabet and Meta to poach consumer data from their publishing rivals degrades competition in digital advertising market, which degrades the digital content ecosystem in which consumers live, work, and play. Former ad-tech entrepreneur Dina Srinivasan wrote in 2019 that "Facebook increasingly knew as much about *The Wall Street Journal's* readers as the *Journal* did itself. Furthermore, unlike the *Journal*, Facebook now knew which *Journal* readers were avid ESPN readers, giving it the capability to bundle and sell targeted audiences, which further commoditized the value of competitors' inventory."[40] In other words, data poaching allowed Meta to drain advertising dollars away from *The Wall Street Journal*. This effect is replicated everywhere. Data poaching allows Alphabet and Meta to capture an increased amount of advertising revenue, which would otherwise flow to independent publishers absent data poaching. The drain from independent publishers reduces consumer choice. A 2020 report from the Competition and Markets Authority in the United Kingdom found that "[w]eak competition in search and social media leads to reduced innovation and choice and to consumers giving up more data than they would like. Weak competition in digital advertising increases the prices of goods and services across the economy and undermines the ability of newspapers and others to produce valuable content, to the detriment of broader society."[41] Draining advertising revenues away from publishers ultimately degrades the services they offer, which harms consumers because it degrades the digital content they use.

Second, mass surveillance imposes a psychological cost on Americans, as there is no clear consumer expectation regarding who is collecting their data. The in-kind, quid-pro quo exchange of consumer data for waiving monetary fees in whole or in part for access to services can mutually benefit both parties, but each party must understand the nature of the exchange. The data collection techniques that the dominant platforms employ extend far beyond the scope of the consumer's knowledge and understanding. As a result, surveys indicate that consumers feel exploited and powerless.

A 2021 survey of global internet users revealed that 86 percent of respondents felt that personal data privacy is a growing concern for them, but 76 percent of respondents said that it was too hard for them to understand how their data are being used by companies. [42] Another 2021 survey showed that 86 percent of U.S. respondents felt data privacy is a growing concern, and 40 percent don't trust

---

[40] Case Against Facebook at 72.

[41] *Online platforms and digital advertising,* COMPETITION & MARKETS AUTHORITY (Jul. 1, 2020), at 5, *available at* https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf.

[42]*Building Consumer Confidence Through Transparency and Control*, CISCO (2021), at 4, *available at* https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf.

companies to use their data ethically.[43] Another 2021 survey revealed that more than half of the consumers surveyed were concerned that their data could be sold, a core business practice of many companies that collect consumer data.[44] Consumers have a reason to be worried—the same survey showed that 29 percent of business leaders surveyed "openly acknowledged that their company sometimes uses unethical data-collection methods."[45] Consumer data was shared with third parties by more than half of the mobile apps in the iOS app store, including Instagram and YouTube, which shared 79 percent and 42 percent of user data, respectively.[46] Similarly, a 2019 Pew Research survey found that 62 percent of Americans did not believe it was possible to go through daily life without having their data collected, 81 percent felt they had no control over the data companies collect, and 79 percent were concerned about how that data was used.[47]

Surveilling a consumer's activity across the web, over products and services owned by separate legal entities, is an abuse of the narrow quid pro quo that consumers understand. Without a clear consumer expectation, consumers are unable to truly know what types of data they are consenting to share, and aggregation enables the dominant tech platforms to learn consumers' most private habits, even offline and without their consent.

B.   How a "Data Poaching" Rule Would Work

The intent of our proposed data poaching rule is to prevent the dominant tech platforms from using their embeds to fully track consumers across the internet without compensating the digital properties that generate the first-party consumer data. The rule *would grant the company with which the consumer interacts the exclusive right to all first-party consumer data created*—that is, this rule would ensure that the quid pro quo of "service for data" is between the consumer and the company with which they interact, creating a clear consumer expectation of who collects their data.[48] Under the data poaching rule, third parties could still temporarily collect and process consumer data in accordance with the service they are providing the rights holder, but they could not retain this data for other commercial purposes.

---

[43] Orson Lucas, Martin Sokalski, and Rob Fisher, *Corporate data responsibility*, KPMG (Aug. 2021), at 1, *available at* https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2021/corporate-data-responsibility-bridging-the-consumer-trust-gap.pdf.

[44] *Id.* at 2.

[45] *Id*. at 3.

[46] Ivan Dimitrov, *Invasive apps*, PCLOUD (Mar. 5, 2021), *available at* https://www.pcloud.com/invasive-apps.

[47] *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER (Nov 15, 2019), *available at* https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[48] Note that while this data poaching rule solves the issue of who is allowed to collect consumer data, by itself the rule does not mandate that the collecting firm inform or otherwise ask consent from consumers if it subsequently sells their data. This discussion is outside the scope of this comment.

The company the consumer interacts with is meant to be understood as the legal entity that owns the service or product that the consumer is using.[49] This rule has no implication for the use of the collected first-party data afterwards. For example, first-party consumer data generated from a digital property may still be internally transferred, externally sold, or used for the purposes of selling targeting advertising. Nor is the rule intended to have any implication for a publisher's use of additional third-party data to augment their first-party data. Under this rule, after its collection a publisher can use its first-party data as it sees fit.

The proposed rule disciplines the ability of the dominant tech platforms to collect consumer data *automatically and passively* from their embeds. If the dominant tech platforms want access to the same first-part consumer data after the rule change, they would (like any other company) need to reach a *separate arrangement* with the independent publisher to purchase that data. To prevent Alphabet or Meta from simply amending their embeds' terms of service contract to automatically enforce transfer after the rule change, the rule would need to explicitly require that any agreement concerning the transfer of rights to first-party data occur as a separate standalone agreement—that is, outside of the terms of use of an embed. This would force the dominant platforms to negotiate (like every other company) for the fair market value of the first-party data.

Returning to the e-bike website example, this rule would preclude Google AdSense from poaching a user's "e-bike interest" from the hypothetical website. Google AdSense would still process and serve the user a related advertisement relevant to the website (earning their standard ad-stack fees in the process), but Alphabet would no longer be able to record the user's e-bike interest after the AdSense processing is complete. Because the e-bike website now *owns* the right to the first-party datapoint of e-bike interest for that user, when a manufacturer seeks to place an ad for a new e-bike model, those advertising dollars would flow to the website rather than Alphabet. If Alphabet wished to purchase the website's user list with an interest in e-bikes, the website would reach a separate agreement for the value of that data.

This rule would *not* prevent Alphabet or Meta from competing in the market for digital advertising using their vast first-party data generating digital properties. For example: Alphabet could sell search ads based on a consumer's search history on Google Search, activity on the Android OS, or through a consumer's use of Google Chrome. But Alphabet could not augment that consumer's advertising profile with app usage data obtained from independent apps through Google Admob. Similarly, Meta could sell ads based on a user's activity on Facebook and Instagram augmented with additional data from the Meta Pixel program, but that Meta Pixel data would only come from independent publishers who have signed a separate agreement with

---

[49] In the event the legal entity that controls the product or service is itself a subsidiary, the parent company would have the right to the data in the same way it has the right to all other assets of the subsidiary.

Meta.[50]

C.   Costs and Benefits of a Data Poaching Rule

The costs of a data poaching rule would be borne by the dominant tech platforms, since they are the entities primarily engaged in data poaching. The benefits, by contrast, would be felt by virtually all competitors and consumers in digital advertising market and related ecosystems. Below, we estimate the magnitude of the cost of the rule to Alphabet and Meta would be approximately ten percent of their digital advertising revenues. We argue that users would benefit directly through enhanced privacy and reduced harm from data breaches. We then explain that that consumers would benefit indirectly through the lowering of online subscription prices because of the increased advertising revenues flowing to independent publishers.

1.   Costs: The Dominant Platforms' Consumer Data Would Become Less Valuable to Advertisers

A data poaching rule would unwind the ability of the dominant tech platforms to poach first-party consumer data from independent digital properties, appropriately limiting the dominant tech platform's first-party data collection to the constellation of properties they own.

The rule would force Alphabet and Meta to compete against third-party publishers for advertising dollars on more equal footing. Alphabet and Meta would be competing against publishers on the basis of the content and services they provide, not on the basis of their market power in related markets.

Such a change would imply a loss of advertising efficiency for the dominant tech platforms, in that it would take more advertising inventory (impressions or views) to generate the same number of clicks. This, in turn, would make Alphabet and Meta's first-party data *relatively* less valuable in the eyes of advertisers than it is today.

A relative diminution of the value of Alphabet's and Meta's consumer data would, at the margin, lead advertisers to spend a larger portion of their advertising budgets with independent publishers. The exact degree of this cost would only be known by Alphabet or Meta, but an approximate order of magnitude can be estimated

---

[50] The rule would need to clearly denote what data can be collected when a consumer passes through multiple layers of ownership. For example, consumer activity within a mobile app on an Android phone would be owned by the app owner, and not Android. However, Android could still collect data that the mobile app is installed and used—just not what occurs within it. Similarly, Single Sign-On integrations would not be able to track consumer activity on an independent digital platform after the initial sign in was authenticated, but they could track that a consumer's use of a Single Sign-On on another digital property.

using a previous event following a similar change in the ability for Meta to track consumers across digital properties on the Apple iPhone.

In February 2022, Meta claimed it would face a projected (global) $10 billion decrease in its digital advertising revenue due to Apple's recently introduced "App Tracking Transparency" feature. The feature allowed iPhone users to limit advertisers from accessing their iPhone user identifier, degrading the ability of Meta to track consumer activity across apps run on the iOS platform.[51] Because Meta's (global) digital advertising revenues from 2021 were $114.9 billion, a $10 billion reduction represents an 9.1 percent loss in revenues.[52] In other words, the loss of the ability to track iPhone user behavior using third parties resulted in an approximate loss of ten percent of Meta's digital advertising revenues.

We believe our proposed rule would have a similar order-of-magnitude effect, on the grounds that it would engender the same end result: Losing access to data poached from independent digital properties.

2. Direct Consumer Benefits: Clear Consumer Expectations, Less Harmful Data Breaches

Consumers feel exploited under the current system and feel they have no control over their data. There is no current consumer expectation with regard to who collects their data. This rule would create that expectation: User data are only being collected by the party with which they enter the quid pro quo agreement. We cannot place a direct economic value on the enhanced trust this may bring, but we will note that "corporate responsibility" and "consumer trust" are heavily studied topics by businesses and consulting firms.[53]

---

[51] Kif Leswing, *Facebook says Apple iOS privacy change will result in $10 billion revenue hit this year*, CNBC (Feb. 2, 2022), *available at* https://www.cnbc.com/2022/02/02/facebook-says-apple-ios-privacy-change-will-cost-10-billion-this-year.html. *See also* Jason Cross, *What is App Tracking Transparency and how do you block app tracking?*, MACWORLD (Apr. 29, 2021), *available at* https://www.macworld.com/article/344420/app-tracking-transparency-privacy-ad-tracking-iphone-ipad-how-to-change-settings.html.

[52] S. Dixon, *Meta: advertising revenue worldwide 2009-2021*, STATISTA (Jul. 27, 2022), *available at* https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/#:~:text=In%202021%2C%20Meta%20(formerly%20Facebook,U.S.%20dollars%20in%20ad%20revenues.

[53] For example, the KPMG surveys cited earlier in this report were administered to determine corporate data responsibility and consumer trust. *See* Orson Lucas, Martin Sokalski, and Rob Fisher, *Corporate data responsibility*, KPMG (Aug. 2021), *available at* https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2021/corporate-data-responsibility-bridging-the-consumer-trust-gap.pdf. Other management consulting firms such as Deloitte study consumer trust of tech firms explicitly. Michael Bondar, Natasha Buckley, Roxana Corduneanu, David Levin, *Quantifying customer trust*, DELOITTE (Jun. 28, 2022), *available at* https://www2.deloitte.com/us/en/insights/industry/technology/customer-trust-technology-sector.html.

Future data breaches are all but assured. Both Alphabet[54] and Meta[55] have had consumer data fall into the hands of nefarious actors who would exploit it for their gain, and there is no reason to believe that perfect data security will exist in the future. A data poaching rule would mitigate the damage to individual consumers relative to the current world where a consumer's data from all over the internet is aggregated and retained in these platforms.

3. Indirect Consumer Benefits: Lower Prices, Greater Social Benefits

i. A More Competitive Digital Advertising Market Would Shift Advertising Dollars Away from the Dominant Tech Platforms and Towards Independent Publishers

As noted above, a data poaching rule would essentially force Alphabet and Meta to compete for advertising dollars against publishers on a level playing field. The rule would increase the relative value of the first-party data collected by publishers relative to the dominant platforms, shifting marginal advertising dollars from the dominant platforms (who currently account for approximately half of all digital advertising spending in the United States) towards publishers.

We can estimate the approximate shift of advertising revenues to publishers. Given the approximate nature of the input data, these figures should be viewed as directional rather than definitive. These calculations are shown in the Appendix.

We first assume the decline in Alphabet's and Meta's digital advertising spending or revenues as a result of the rule. We use the value of (approximately) ten percent lower digital advertising revenues from Meta's statement after the iOS privacy changes discussed above. We recognize that advertising *revenues* are different than advertising *spending*, because publishers receive, on average, approximately 65 percent of each advertising dollar spent, with the remaining collected by the ad-stack middlemen. [56] (Another estimate places the ultimate publisher take rate at 28 to 40 percent, depending on the amount of fraudulent traffic and fraudulent clicks.[57]) Nevertheless, because Meta's "$10 billion loss" claim was

---

[54] Michael X. Heiligenstein, *Google Data Breaches: Full Timeline Through 2022*, FIREWALL TIMES (Jan. 18, 2022), *available at* https://firewalltimes.com/google-data-breach-timeline/.

[55] Issie Lapowsky, *The 21 (and Counting) Biggest Facebook Scandals of 2018*, WIRED (Dec. 20, 2018), *available at* https://www.wired.com/story/facebook-scandals-2018/; Issie Lapowsky, *In Latest Facebook Data Exposure, History Repeats Itself*, WIRED (Apr. 3, 2019), *available at* https://www.wired.com/story/facebook-apps-540-million-records/.

[56] *Online platforms and digital advertising,* COMPETITION & MARKETS AUTHORITY (Jul. 1, 2020), at 65, *available at* https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf.

[57] Mikko Kotila, Ruben Cuevas Rumin, Shailin Dhar, *Compendium of ad fraud knowledge for media investors*, WORLD FEDERATION OF ADVERTISERS (Jun. 2, 2016), at 12, *available at* https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjWt-

with regard to *revenues* and was compared to their global *revenues*, we assume that the ad-stack take rate is fixed, meaning a ten percent decrease in revenues implies a ten percent decrease in advertising spending.[58]

Next, we estimate U.S. total digital advertising spending and Alphabet's and Meta's shares of this total. According to figures from eMarketer, U.S. digital advertising spending in 2021 was $211.20 billion, and Alphabet and Meta accounted for 28.6 percent and 23.8 percent of that spending respectively. Of the remaining spending, Amazon took 11.6 percent, and all other publishers took 36 percent. Accordingly, we estimate that Alphabet and Meta account for $60.4 billion and $50.3 billion of U.S. digital advertising spending in 2021 respectively. A ten percent reduction of both yields reduction $6.04 billion and $5.03 billion respectively, or a $11.07 billion spending reduction in total.

We assume that total U.S. advertising spending would *not* decrease following the rule change,[59] but would instead be channeled at the margin to other competitors in digital advertising market based on their current market shares. We thus allocate the $11.07 billion from Alphabet and Meta to the remaining market participants, which include all publishers, inclusive of larger firms such as Amazon, Apple, Netflix, and Hulu. Using all other publisher's 2021 market shares as a weight, this would imply $2.7 billion in additional advertising spending transferring to Amazon specifically (Amazon is the only other firm with named market share in this dataset), and $8.4 billion in additional advertising spending transferring to all other publishers.

Relative to their pre-transfer share of spending, this ten percent reduction in Alphabet and Meta spend would result in an approximate eleven percent increase in digital advertising spending on all other publishers.[60] Assuming the same conversion rates of advertising spending into publisher revenue, this would imply an eleven percent increase in all other publishers' advertising revenues.[61]

KI27v6AhUFJn0KHee2BboQFnoECA0QAQ&url=https%3A%2F%2Fwww.wfanet.org%2Fadfraud&usg=AOvVaw0pmACZitmLv38X7XIi2CVg.

[58] While Alphabet and Meta are the primary firms that use embeds to poach and monetize consumer data, to the extent that other firms engage and profit from data poaching, we would expect those revenues to be similarly impacted. We believe this is desirable, as data poaching by definition does not have a procompetitive justification.

[59] According to projections from eMarketer, U.S. digital ad spending is projected to linearly increase to over $300 billion by 2025. Sara Lebow, *Google, Facebook, and Amazon to Account for 64% of US Digital Ad Spending This Year,* INSIDER INTELLIGENCE (Nov. 3, 2021), *available at* https://www.insiderintelligence.com/content/google-facebook-amazon-account-over-70-of-us-digital-ad-spending.

[60] *See* the Appendix for these calculations.

[61] This ratio of 1 to approximately 1.1 holds if the actual decline of Alphabet and Meta's digital advertising spending or revenues is more or less than ten percent. For example, a more conservative digital advertising spending decline of 1, 3, and 5 percent for Alphabet and Meta would be associated with a gain for all other publishers of 1.1, 3.3, and 5.5 percent, respectively.

ii. Revenue Shifting to Publishers With Paying Consumers Puts Downward Pressure on Consumer Prices

Online publishers who both advertise to consumers and charge consumers for access engage in two-sided pricing: A publisher offers original content or services to consumers for one price and offers advertisers access to those consumers for another price.

Economic theory shows that for firms that use a two-sided pricing model, upward pressure on price to one set of customers leads to downward pressure on price to the other customers.[62] Intuitively, publishers perceive additional advertising revenue as a subsidy for the cost of producing content for customers; when the net cost of producing content falls (equal to the cost of production less advertising revenue), basic economics predicts that the price of such content falls. This "seesaw principle" implies that gains from one set of customers subsidizes the other participants.[63]

The trade-off between advertising revenues for subscription fees is plain to see in practice. At one extreme, customers pay a price of zero for digital content but are subject to advertisements. At the other extreme, some publishers allow consumers to opt-out of viewing ads entirely by paying a one-time or subscription price. For example, a Spotify free account is subject to frequent ad breaks, but a paid subscription removes ads entirely.[64]

For online publishers who charge consumer fees but *also* display digital ads, an influx of advertising revenues "tilts" the seesaw towards a lower consumer fee price point. This is not done out of generosity: Online publishers can expect greater overall profits if they do so. The two-sided pricing model developed by economists Jean-Charles Rochet and Jean Tirole demonstrates this phenomenon.[65] In a two-sided market, a firm's profit maximizing *total* price (the sum of the consumer and the advertiser prices) is determined by the sum of the demand elasticities on both the consumer and advertiser side.[66] Thus, without changing the underlying demand elasticities, an increase in the advertise "price" (more digital ad revenues for the same number of users as a result of the rule) incentivizes the publisher to drop its consumer price. Doing so brings in additional users and achieves the profit

---

[62] *See, e.g.,* Kevin Caves & Hal Singer, *Competing Approaches to Antitrust: An Application in the Payment Card Industry,* 26(3) GEORGE MASON LAW REVIEW (2014).

[63] Jean-Charles Rochet & Jean Tirole, *Two-Sided Markets: A Progress Report*, 37 RAND J. ECON. 645, 659 (2006) ("The linkage between the two sides comes from the reinterpretation of costs as opportunity costs. The linkage also shows up in the form of a simple 'seesaw principle': a factor that is conducive to a high price on one side, to the extent that it raises the platform's margin on that side, tends also to call for a low price on the other side as attracting members on that other side becomes more profitable.").

[64] *Premium plans*, SPOTIFY, *available at* https://support.spotify.com/us/article/premium-plans/.

[65] Jean-Charles Rochet & Jean Tirole, *Platform Competition in Two-Sided Markets*, 1(4) EUROPEAN ECONOMIC ASSOCIATION 990-1029, (2003).

[66] *Id.* at 997, equations 2-4.

maximizing total price. [67] This framework has been widely cited by other economists.[68]

iii. Revenue Shifting to News Outlets Incentivizes Investment in New News Content

A permanent influx of revenue would prompt additional investment in original content creation. Economic theory predicts that, as two-sided platform revenues are a function of the number of users on both sides of the platform, publishers would be incentivized to reinvest any revenue increase resulting from the rule to producing more original content to attract yet more consumers (and thus more advertising spending).

This is also true for original content creators such as news outlets. News sources are generally understood to provide social benefits in a free and fair society.[69] Thus, a shift of advertising revenues to news publishers would engender greater investment in news itself, which benefits American civil society generally.

Question 41: A Data Poaching Rule Would Have a Little Effect on First- or Third-Party Targeting

Question 41 asks: "To what alternative advertising practices, if any, would companies turn in the event new rules somehow limit first- or third-party targeting?"

Answer: The proposed data poaching rule would have no direct implications for the collection or use of first- and third-party data for the company that attracted the consumer to the service or product in the first place. It would not require companies to turn to any alternative advertising practices. The rule would remedy a current abuse in the collection of first-party data. Compared to the current world, a data poaching rule will put greater importance on the first-party data of independent companies, directly benefiting these original content creators.

---

[67] *Id.* "Proposition 1. (i) a monopoly platform's total price, $p = p^b + p^s$, is given by the standard Lerner formular for elasticity equal to the sum of the two elasticities, $n = n^b + n^s: \frac{p-c}{p} = \frac{1}{n}$."

[68] *See, e.g.*, Marc Rysman, *The Economics of Two-Sided Markets*, 23(3) JOURNAL OF ECONOMIC PERSPECTIVES 125-43, (2009); Avi Goldfarb and Catherine Tucker, *Digital Economics*, 57 JOURNAL OF ECONOMIC LITERATURE 3-43, (2019); Joseph Farrell & Paul Klemperer, *Coordination and lock-in: Competition with switching costs and network effects,* in MARK ARMSTRONG AND ROBERT PORTER EDS., 3 HANDBOOK OF INDUSTRIAL ORGANIZATION (Elsevier 2007).

[69] *See, e.g., Journalism as a public good,* 2021, UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION, *available at* https://www.unesco.org/reports/world-media-trends/2021/en/journalism-public-good; Annabelle Woodward, *Study Finds Vast Majority of Americans See Local News As A 'Public Good',* FORBES (Nov. 18 2019), *available at* https://www.forbes.com/sites/annabellewoodward1/2019/11/18/study-finds-vast-majority-of-americans-see-local-news-as-a-public-good/?sh=3b37cbcc242e.

Question 43: A Data Poaching Rule Imposes No Limitations on the Use of Correctly Collected First-Party Data

Question 43 asks: "To what extent, if at all, should new trade regulation rules impose limitations on companies' collection, use, and retention of consumer data? Should they, for example, institute data minimization requirements or purpose limitations, *i.e.,* limit companies from collecting, retaining, using, or transferring consumer data beyond a certain predefined point? Or, similarly, should they require companies to collect, retain, use, or transfer consumer data only to the extent necessary to deliver the specific service that a given individual consumer explicitly seeks or those that are compatible with that specific service? If so, how? How should it determine or define which uses are compatible? How, moreover, could the Commission discern which data are relevant to achieving certain purposes and no more?"

Answer: Adopting this rule would explicitly codify the quid pro quo relationship between consumers and companies. Consumers would know that the only entity collecting their activity data is the one they are engaging with on the service or product they are using. [70] It requires no further limitation for data collection or transmission.

Question 44: A Data Poaching Rule is Agnostic to Data Retention

Question 44 asks: "By contrast, should new trade regulation rules restrict the period of time that companies collect or retain consumer data, irrespective of the different purposes to which it puts that data? If so, how should such rules define the relevant period?"

Answer: A data poaching rule unwinds the primary harms of commercial surveillance with enhanced competition and greater data collection transparency. Under a data poaching rule, there would be no need to restrict the period of time that companies collect or retain user data.

Question 45: A Data Poaching Rule Is Largely Self-Enforcing and Technically Straightforward to Audit

Question 45 asks: "Pursuant to a purpose limitation rule, how, if at all, should the Commission discern whether data that consumers give for one purpose has been only used for that specified purpose? To what extent, moreover, should the Commission permit use of consumer data that is compatible with, but distinct from, the purpose for which consumers explicitly give their data?"

Answer: Using the proposed rule above, the Commission grants the "right" of

---

[70] Note, however, that if the user was using a Google phone or web browser (Google Chrome), their activity could still be collected from this source.

data collection to the firm owning the service or product. If Alphabet or Meta violates that "right" by inappropriately poaching consumer data after the rule change, the firm whose "right" was violated would have legal recourse against the offending company, which could be accompanied by FTC fines once proven.

Because it would be in the self-interest of the independent firms to enforce the rule via litigation, the FTC would likely not need to spend time and money actively enforcing this rule. However, if the FTC is still concerned that companies are not in compliance with a data poaching rule, it could audit the main embeds run by Alphabet and Meta across the internet to ensure that they are not poaching first-party data.

Question 46: A Data Poaching Rule Can be Industry Agnostic

Question 46 asks: "Or should new rules impose data minimization or purpose limitations only for certain designated practices or services? Should, for example, the Commission impose limits on data use for essential services such as finance, healthcare, or search—that is, should it restrict companies that provide these services from using, retaining, or transferring consumer data for any other service or commercial endeavor? If so, how?"

Answer: A data poaching rule focuses on how data are collected, ensuring that consumers know exactly what data they are giving up and where. With this approach, there is no need to create industry-specific limits on data use.

Question 47: A Data Poaching Rule Minimizes the Harm From Data Breaches

Question 47 asks: "To what extent would data minimization requirements or purpose limitations protect consumer data security?"

Answer: As we explain in above in **Q39.C.2**, the data poaching rule would prevent the dominant tech platforms from "fully tracking" individual consumers across the internet. The rule mechanically ensures that only a portion of a consumer's total online footprint is exposed in any future data breach from those dominant tech platforms.

Appendix

ESTIMATED INDEPENDENT PUBLISHER REVENUE INCREASES

#	Company	Shares	Equation
[1]	Alphabet	28.6%	Input
[2]	Meta	23.8%	Input
[3]	Amazon	11.6%	Input
[4]	Other Publishers	36.0%	Input
	U.S. Digital Ad Spend		
[5]	**Total**	**$211,200,000,000**	**Input**
[6]	Alphabet	$60,403,200,000	[1] * [5]
[7]	Meta	$50,265,600,000	[2] * [5]
[8]	Amazon	$24,499,200,000	[3] * [5]
[9]	Other Publishers	$76,032,000,000	[4] * [5]
	Reduction of 10%		
[10]	Alphabet	$6,040,320,000	[6] * 0.1
[11]	Meta	$5,026,560,000	[7] * 0.1
[12]	Total	$11,066,880,000	[10] + [11]
	Redistribution		
[13]	To Amazon	$2,696,970,756	[12] * [8]/([8]+[9])
[14]	To Other Publishers	$8,369,909,244	[12] * [9]/([8]+[9])
[15]	*Percent Increase*	11.01%	[14] / [4]

Source: Sarah Lebow, *Google, Facebook, and Amazon to account for 64% of US digital ad spending this year*, INSIDER INTELLIGENCE (NOV. 3, 2021), *available at* https://www.insiderintelligence.com/content/google-facebook-amazon-account-over-70-of-us-digital-ad-spending.