

**Before the Federal Trade Commission  
Response to Request for Information on Commercial Surveillance  
Docket ID FTC-2022-0053**

**Written Comments from the American Economic Liberties Project  
and the Center for Digital Democracy  
November 18, 2022**

The American Economic Liberties Project is a nonprofit research and advocacy organization dedicated to understanding and addressing the problem of concentrated economic power in the United States. The Center for Digital Democracy is a nonprofit organization using education, advocacy, and research into commercial data practices to ensure that digital technologies serve and strengthen democratic values, institutions, and processes. We are submitting this comment in response to the advance notice of proposed rulemaking regarding whether and how the Federal Trade Commission should implement regulations “concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair and deceptive.” The attached appendix provides a proposed rule prohibiting surveillance advertising and clarifying which practices fall under the rule and are violations of it.

**I. INTRODUCTION**

Surveillance advertising is the practice of extensively tracking and profiling individuals and groups, and then microtargeting them based on their behavioral history, relationships, and identity for advertising. It allows dominant firms to (1) extract data from captive user bases which would not otherwise remain users but for

the market power of those firms; (2) monetize that data through targeting techniques that rely on the resources and scale from the platforms' market power; and (3) integrate this data and resource advantage across business lines, which in turn allows dominant platforms to entrench existing power and leverage it into greater power elsewhere.

Beyond these descriptive facts about surveillance advertising, we agree with the basic state of affairs described in Accountable Tech's September 2021 Petition for Rulemaking to Prohibit Surveillance Advertising to the Commission.<sup>1</sup> The business model for surveillance advertising constitutes an unfair method of competition. Surveillance advertising allows dominant firms to (1) extract data from captive user bases which would not otherwise remain users but for the market power of those firms, (2) monetize that data through targeting techniques that rely on the resources and scale from the platforms' market power, and (3) integrate this data and resource advantage across business lines which allows dominant platforms to entrench existing power and leverage it into greater power elsewhere.

We have reached an inflection point in the development of advertising and data privacy standards which makes it uniquely important for the FTC to publish a clear rule banning surveillance advertising. The European Union and states such as California are more strictly regulating data practices; Apple and Mozilla are imposing

---

<sup>1</sup> Accountable Tech, Petition for Rulemaking to Prohibit Surveillance Advertising, Before the Federal Trade Commission (Sept. 23 2021), *available at* <https://accountabletech.org/wp-content/uploads/Rulemaking-Petition-to-Prohibit-Surveillance-Advertising.pdf> (last accessed Oct. 24, 2022).

stricter limits on third party cookies and data trackers; and Google plans to eliminate third party trackers in Chrome by the end of 2024.<sup>2</sup> This has spurred the development of an array of proposed and emerging approaches for how data can be used to determine someone’s identity for online advertising.<sup>3</sup>

At this critical inflection point, the Commission must clarify the allowable scope of competitive behavior. Restricting commercial surveillance will prevent current dominant platforms from further entrenching their market power and prevent U.S. advertisers, publishers, and consumers from wasting time and resources on approaches that unfairly favor the largest platforms at the expense of privacy and consumer protection.<sup>4</sup> Claims by tech leaders such as Google and Meta that their data

---

<sup>2</sup> Matt Southern, “Google Gives Third-Party Cookies Another Year,” Search Engine Journal (July 28, 2022), *available at* <https://www.searchenginejournal.com/google-gives-third-party-cookies-another-year/459412/> (last accessed Oct. 5, 2022).

<sup>3</sup> Sarah Sluis, “Confused About Identity? This List of 80 Identity Partners May (Or May Not) Help,” Ad Exchanger (Apr. 12, 2021), *available at* <https://www.adexchanger.com/online-advertising/confused-about-identity-this-list-of-80-identity-partners-may-or-may-not-help/> (last accessed Oct. 13, 2022); “The Long Goodbye,” Digiday (Sept. 2021), *available at* <https://digiday.com/marketing/the-long-goodbye/> (last accessed Oct. 3, 2022); User Privacy and Data Use, Apple, *available at* <https://developer.apple.com/app-store/user-privacy-and-data-use/> (last accessed Oct. 3, 2022).

<sup>4</sup> For example, privacy experts and online marketing competitors have raised questions about the efficacy of Google and other similar industry-led proposals involving new ways to target individuals or their devices using various methods to replace cookies. “The Evolution of Customer Journey Management,” Winterberry Group (2021), *available at* <https://www.winterberrygroup.com/insights-library/the-evolution-of-customer-journey-management-2021-pxe9t> (last accessed Oct. 13, 2022); Jeff Chester, “The Whole World Will Still be Watching You: Google & Digital Marketing Industry “Death-of-the-Cookie” Privacy Initiatives Require Scrutiny from Public Policymakers,” Center for Digital Democracy (Feb. 18, 2021), *available at* <https://www.democraticmedia.org/article/whole-world-will-still-be-watching-you-google-digital-marketing-industry-death-cookie> (last accessed Oct. 13, 2022); Jeff

collection reforms are aimed at privacy and not profit simply do not pass the smell test. For example, in response to privacy concerns, Google announced that it would no longer use third-party cookies to track users, and that it planned to replace them with an alternative algorithmic system to track individual users—initially “FLOC” (Federating Learning of Cohorts) and rebranded as “Topics.”<sup>5</sup> Its proposal would replace old privacy risks with new ones, as the ultimate outcome of this new method—being profiled, tracked, and targeted based on online behavior – does not go away. As long as Big Tech is allowed to engage in surveillance advertising, it will monetize and manipulate internet user data to grow and exert its dominance over internet advertising at the expense of consumers, small businesses, and publishers.

Surveillance advertising depends on the substantial collection of data from individuals and groups of individuals across a wide variety of sources, and the use of that data to target advertisements creates a substantial revenue stream, combined with the flywheel effects of data collection, data analytics, and market power enjoyed by the dominant platforms. At the same, viable alternative technologies exist for

---

Chester, “Cookie Wars: How New Data Profiling and Targeting Techniques Threaten Citizens and Consumers in the ‘Big Data’ Era,” *European Data Protection in Good Health?* (Feb. 22, 2012), *available at* [https://link.springer.com/chapter/10.1007/978-94-007-2903-2\\_4](https://link.springer.com/chapter/10.1007/978-94-007-2903-2_4) (last accessed Oct. 13, 2022).

<sup>5</sup> Kate O-Flaherty, “Google Says It Wants A Privacy First Web, Here’s What That Really Means,” *Forbes* (March 7, 2021), *available at* <https://www.forbes.com/sites/kateoflahertyuk/2021/03/07/google-says-it-wants-a-privacy-first-web-heres-what-that-really-means/?sh=404d3ae1bfb> (last accessed Oct. 13, 2022). Vinay Goel, “Get to know the new Topics API for Privacy Sandbox,” *Google* (Jan. 25, 2022), *available at* <https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/> (last accessed Nov. 15, 2022).

targeted advertising that do not depend on mass commercial surveillance. We therefore propose a wholesale ban on individual data collection for the purpose of algorithmically or otherwise automatically targeting individuals or segments of individuals as recipients of online advertising and marketing.<sup>6</sup> Such a rule would serve the dual purpose of protecting internet users' privacy interests and preventing commercial surveillance's inevitable structural tendency to create market dominance.

## II. THE SURVEILLANCE ADVERTISING MONSTER

Surveillance advertising relies on the collection of extensive and intimate data on individuals, families, and communities to display advertisements targeted to those groups on the websites they visit and through the online services they use. The historic failures of the Commission to address the development of programmatic advertising, the dominant role of mobile devices, and the emergence and operations of omnichannel targeting have unleashed an interconnected host of data brokers, data marketing clouds, geo-location information providers, advertising networks, data management platforms trading desks, and consumer "identity" firms which provide (often in real-time) vast material for personalized digital dossiers, which is the combination of all online data collected about an individual.<sup>7</sup> These dossiers include

---

<sup>6</sup> Proposed text for this proposed rule and illustrations of its use are set forth in the attached appendix.

<sup>7</sup> AWS Data Exchange, Amazon Web Services, *available at*, <https://aws.amazon.com/data-exchange/> (last accessed Oct. 13, 2022); Nielsen Marketing Cloud, Nielsen, *available at* <https://www.nielsen.com/solutions/media-planning/marketing-cloud/> (last accessed Oct. 13, 2022); Marketing Solutions, Neustar, *available at* <https://www.home.neustar/marketing-solutions> (last accessed

information about a person’s financial status, health concerns, ethnicity/race, presence of children, spending behaviors online and offline, personal interests, geolocational history, and thousands of other categories. The largest platforms, which capture a lion’s share of data on individuals and others across their various services, are especially able to leverage those collections to maintain their dominance. For example, the Google Marketing Platform provides tools, including “Big Data” enriched analysis, in a cloud that facilitates continuous cross application and device ad targeting.<sup>8</sup> Facebook and Amazon maintain a similar data-enriched surveillance advertising infrastructure as well, that—as with Google—continually expands in scope and impact.<sup>9</sup>

Today, the Big 3 credit bureaus (Experian, TransUnion, and Equifax) have been transformed into providers of extensive consumer information for online surveillance marketing.<sup>10</sup> Marketing “clouds” have assembled a myriad of data

---

Oct. 13, 2022); Identity Resolution, LiveRamp, *available at* <https://liveramp.com/our-platform/identity-graph/> (last accessed Oct. 13, 2022).

<sup>8</sup> “Meeting the Data Challenge, How to Drive Growth with Google Marketing Platform + Google Cloud,” Google, *available at* <https://services.google.com/fh/files/misc/meeting-the-data-challenge-with-google-marketing-platform-and-google-cloud.pdf> (last accessed Nov. 29, 2021); Meta for Developers: Marketing API, Facebook, *available at* <https://developers.facebook.com/products/marketing-api/> (last accessed Nov. 27, 2021).

<sup>9</sup> Amazon DSP, Amazon, *available at* <https://advertising.amazon.com/solutions/products/amazon-dsp> (last accessed Nov. 30, 2021).

<sup>10</sup> Product Sheet, “OmniActivation Strategic Services,” Experian, *available at* <https://www.experian.com/content/dam/marketing/na/assets/ems/marketing-services/documents/product-sheets/omniactivation-strategic-services.pdf> (last accessed Nov. 29, 2021); Press Release, “TransUnion Introduces TruAudience

sources which can be quickly downloaded and used for profile-based tracking and targeting, providing one-stop shopping for information on hundreds of millions of people in the United States.<sup>11</sup> There is also a geolocation data complex—supplied by apps, internet service providers, and others—that closely surveils our physical movement from street to street.<sup>12</sup> Information derived from social media interactions with social media are also part of today’s data surveillance system.<sup>13</sup>

This data is collected, analyzed, and used to alter internet users’ behavior. Advertisers can determine how best to penetrate someone’s emotional and unconscious brain functioning; leverage it to deeply personalize content for what’s

---

Marketing Solutions to Power Privacy-Centric Identity and Data Capabilities for Omnichannel Advertising,” TransUnion (Aug. 24, 2021), *available at* <https://newsroom.transunion.com/transunion-introduces-truaudience-marketing-solutions--to-power-privacy-centric-identity-and-data-capabilities-for-omnichannel-advertising/> (last accessed Oct. 13, 2022); Digital Marketing, Equifax, <https://www.equifax.com/business/digital-marketing/>

<sup>11</sup> Oracle Data Management Platform Help Center, Oracle Data Marketplace, Oracle, *available at* <https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/AudienceDataMarketplace/AudienceDataMarketplace.html> (last accessed Nov. 29, 2021); Oracle Advertising: Oracle Data Cloud—Data Providers, Oracle, *available at* <https://www.oracle.com/cx/advertising/data-providers/> (last accessed Nov. 30, 2021); Companies can also leverage these clouds for their own targeting. Meeting Advertising Studio, Salesforce, *available at* <https://www.salesforce.com/products/marketing-cloud/digital-advertising/> (last accessed Nov. 29, 2021).

<sup>12</sup> John Keegan, *There’s a Multibillion Dollar Market for Your Phone’s Location Data*, The Markup (Sept. 30, 2021), *available at* <https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data> (last accessed Oct. 13, 2022).

<sup>13</sup> Social media analytics has long been a method used for ad targeting. For example: Mandy Patterson, *Your Guide to Social Media Targeting Via Sprouting Social* (Oct. 26, 2020) <https://sproutsocial.com/insights/your-guide-to-social-media-targeting-via-sprout/> (last accessed Oct. 13, 2022).

called “engagement”; transform advertising “in-flight” to follow a person regardless of the device they are using and restructure it based on their actions; and identify users’ responses, including minutely measuring how an advertisement triggers the purchase of actual items online or at a store. These are continuous processes operating on a round-the-clock basis without the knowledge or control of the individual.<sup>14</sup> Over the last few years, Google, Facebook, and many other data surveillance marketers have incorporated machine learning and artificial intelligence into their surveilling processes, enabling even faster determinations regarding the use of information for targeted advertising, such as predictive audiences.<sup>15</sup>

---

<sup>14</sup> Neuromarketing Science & Business Association, available at <https://nmsba.com/> (last accessed Nov. 30, 2021); Nielsen Consumer Neuroscience Unveils Behavioral Sciences Institute, PR Newswire (Apr. 1, 2019), available at <https://www.prnewswire.com/news-releases/nielsen-consumer-neuroscience-unveils-behavioral-sciences-institute-300821386.html> (last accessed Oct. 13, 2022); Adobe Experience Platform, Adobe, available at <https://business.adobe.com/products/experience-platform/adobe-experience-platform.html> (last accessed Nov. 29, 2021); *Director Mix: Create Customized Videos at Scale*, Google (June 2021), available at <https://www.thinkwithgoogle.com/future-of-marketing/creativity/tools/director-mix/> (last accessed Nov. 29, 2021); Walmart Connect, Walmart, available at <https://walmartconnect.com/content/wmg/home/solutions.html> (last accessed Nov. 30, 2021).

<sup>15</sup> Jerry Dischler, *Putting Machine Learning into the Hands of Every Advertiser*, Google (June 10, 2018), available at <https://www.blog.google/technology/ads/machine-learning-hands-advertisers/> (last accessed Oct. 13, 2022); Press Release, *Boost Liquidity and Work Smarter with Machine Learning*, Facebook (Mar. 27, 2019), available at <https://www.facebook.com/business/news/insights/boost-liquidity-and-work-smarter-with-machine-learning> (last accessed Oct. 13, 2022); Analytics Help, *Audiences, Remarketing, and User-ID: [GA4] Predictive audiences*, Google, available at <https://support.google.com/analytics/answer/9805833?hl=en> (last accessed Nov. 30, 2021); IBM Watson Predictive Audiences, IBM, available at <https://www.ibm.com/watson-advertising/solutions/ibm-predictive-audiences> (last accessed Nov. 30, 2021).

### III. CONTEXTUAL ADVERTISING AS AN EFFECTIVE ALTERNATIVE TECHNOLOGY

“Contextual advertising” capabilities enable the delivery of relevant marketing without profiling or tracking consumers or collecting their data profiles. With contextual advertising, instead advertising “targets potential customers by relying on context such as the content of a webpage, location or weather,” not based on data collected about their search or other online behavior that was tracked separately.<sup>16</sup> Many of the new technologies deployed for surveillance advertising can also be repurposed for contextual advertising to “match the product intent with the content purpose/emotion/feeling” associated with the site, instead of data collected about individual users visiting the site.<sup>17</sup>

Leading publishers, as well as a significant number of vendors who provide the technological tools to do so, are increasingly using contextual advertising. Comscore, the New York Times, and ad firm Dentsu, to name a few, have developed their own approaches to contextual advertising.<sup>18</sup> In addition, the online marketing industry

---

<sup>16</sup> “What is contextual advertising? Everything you need to know,” IBM Watson Advertising, Sept. 14, 2021, *available at* <https://www.ibm.com/watson-advertising/thought-leadership/what-is-contextual-advertising> (last accessed Oct. 13, 2022).

<sup>17</sup> “How AI & Contextual Advertising Can Help Advertisers in a Cookie-less World,” CatapultX, Nov. 7, 2021, *available at* <https://www.catapultx.com/blog/how-ai-contextual-advertising-in-a-cookie-less-world> (last accessed Oct. 13, 2022).

<sup>18</sup> Contextual Targeting, New York Times, *available at* <https://nytmmediakit.com/contextual-targeting> (last accessed Nov. 29, 2021); Contextual Targeting Solution: Achieve Privacy-Focused and Brand-Safe Cross-Platform Ad Delivery, Comscore, *available at* <https://www.comscore.com/jpn/Products/Activation/Contextual-Targeting-Solution> (last accessed Nov. 30, 2021); “Dentsu UK Launches Proprietary Contextual Data

group Interactive Advertising Bureau has established industry-wide criteria defining contextual related taxonomy categories. In addition, such contextual advertising can be delivered in both an efficient and “brand safe” manner, issues of special importance to many leading advertisers.<sup>19</sup> There is also a growing base of research which illustrates how well contextual approaches deliver compared to current surveillance and programmatic approaches.<sup>20</sup> Contextual advertising will enable the online marketing industry to thrive and publishers to retain and expand their revenues while fostering a variety of approaches that are competitive and offer better privacy. Thus, the prohibition of surveillance advertising as a business model does not eliminate the ability of other industries to effectively advertise or of publishers to sell online advertising space.

---

Platform,” Dentsu (May 20, 2021), <https://www.dentsu.com/uk/en/media-and-investors/dentsu-launches-contextual-intelligence> (last accessed Oct. 13, 2022).

<sup>19</sup> See for example: Oracle Contextual Advertising, Oracle, *available at* <https://www.oracle.com/cx/advertising/contextual-intelligence/> (last accessed Nov. 29, 2021); “Contextual Approach to Targeting Digital Advertising,” iab. Tech Lab (Apr. 8, 2021), *available at* <https://go.iab.com/rs/786-LBD-533/images/Contextual%20APACIv3.0%20small.pdf> (last accessed Oct. 13, 2022); “Understanding Contextual Relevance and Efficiency,” GumGum, *available at* <https://insights.gumgum.com/hubfs/DAN%20Research%20Study/GumGum%20Contextual%20Research%20Paper-1.pdf> (last accessed Nov. 30, 2021); Lucinda Southern, “‘Supercharging Contextual’: Publishers Eye Potential for Contextual Ad Revenue Growth,” Digiday (Sept. 3, 2020), *available at* <https://digiday.com/media/supercharging-contextual-publishers-eye-potential-for-contextual-ad-revenue-growth/> (last accessed Oct. 13, 2022).

<sup>20</sup> Natasha Lomas, “Data from Dutch Public Broadcaster Shows the Value of Ditching Creepy Ads,” TechCrunch (July 24, 2020), *available at* <https://techcrunch.com/2020/07/24/data-from-dutch-public-broadcaster-shows-the-value-of-ditching-creepy-ads/> (last accessed Oct. 13, 2022).

#### **IV. CONCLUSION**

The dangers of commercial surveillance are well documented. Allowing it any form, even if restricted, will still allow a few dominant players to amass and benefit from the massive swaths of data they collect. It could perhaps put them at an even greater advantage because the smaller competitors, to the extent they even exist, will face even bigger hurdles under the new restrictions. As a result, the only real solution is a wholesale ban on the practice, which will restore competition in the world of digital advertising and protect internet users from massive invasions of their privacy.

## **Appendix: Proposed Rule**

Given the many dangers posed by commercial surveillance, American Economic Liberties and the Center for Digital Democracy propose the following rule:

### **Section 1**

Internet information services providers, or an entity acting on their behalves, shall not collect, use, share, or otherwise process individual user data for the purpose of algorithmically or otherwise automatically targeting individuals or segments of individuals as recipients of online advertising and marketing.

Exempted from this rule is the collection, use, and processing of individual user data regarding only (a) email contact information, or (b) a recognized place, so long as that data is not algorithmically or automatically processed together with any other individual user data.

### **Section 2**

(a) Definitions –

- (1) “Internet information services providers” shall include any website, app, or digital property on which any person or organization does business, disseminates information, or interacts with other users.
- (2) “Individual user data” shall include any:
  - (a) information that is personally identifying or otherwise linked to an individual or a personal device;
  - (b) information that is reasonably linkable to an individual or a personal device; or
  - (c) information that is delinked from individual users but nonetheless can be used on its own or in combination with other publicly or privately available information to target individuals or groups of individuals based on the user’s information for the purpose of advertising and marketing.
- (3) “Advertising and marketing” shall mean a communication, technique, and practice employed by a business or a person acting on the business’ behalf in any medium to bring products, services,

opinions, companies or brands, or causes to be noticed for the purpose of persuading the recipient to respond in a manner intended to commercially benefit the advertiser.

(4) “Algorithm” shall mean a computational process that uses machine learning, natural language processing, artificial intelligence techniques, or other computational processing techniques of similar or greater complexity that makes a decision or facilitate human decision making with respect to covered data, including to determine the provision of products or services or to rank, order, promote, recommend, amplify, or similarly determine the delivery or display of information to an individual. “Algorithmically” shall mean by the use or with the assistance of any such algorithm.

(5) “Recognized place” shall mean any of the following:

- (i) a State.
- (ii) Indian lands.
- (iii) A county, municipality, city, town, township, village, borough, or similar unit of general government that is incorporated pursuant to a State law or an incorporated place as defined by the most recent glossary of the Bureau of the Census.
- (iv) A census designated place as defined by the most recent glossary of the Bureau of the Census.
- (v) A designated market area as defined in section 122(j) of title 17, United States Code.
- (vi) A congressional district.

### **Section 3**

This rule shall be effective:

- (1) 12 months following the date of adoption for internet information services providers with over 100,000,000 monthly active users in the United States; and
- (2) 24 months following the date of adoption for all internet information services providers.

### **Illustrations**

- 1. An internet blogger sending emails with blog content to their subscribed readership generally is not a violation. A mailing list with emails attached to other

personally identifying information like names may be considered a collection of individual user data, but collection, use, and processing of individual user data regarding only email contact information is exempted from the rule.

2. A newspaper advertising to its readership generally adjacent to an article on sports is not a violation. A physical newspaper with print advertisements would not fall under the definition of “internet information service provider” that would render the rule applicable. For online editions, the publisher is an information services provider. However, publishing advertisements generally to an entire readership alongside news or editorial content does not constitute prohibited targeting of advertising or marketing based on individual user data. Email or payment information collected to transact for news distribution is not collection of user data for the purpose of advertising because the information is not used for targeted advertising or marketing. Subdividing an online publication and its advertisements in order to target advertisements based on “recognized place,” without collecting, using, or processing any additional user data, is exempted from the rule.

3. In the case of an online magazine company publishing different editions for different readerships—for example for different language readerships, or for different geographic regions, without collecting additional individual user data—there is no violation. The publisher is an internet information services provider and advertisements sent to their users are in the scope of the rule. However, the advertisements are directed without regard to the individual information of said

users. Instead, advertisements are directed a priori by pairing them with content that an audience with relevant interests may find relevant. For example, an outdoor magazine serving an English-speaking audience in Colorado in the winter may advertise ski supplies while a political magazine serving a Spanish speaking audience in California around election season may advertise ballot initiatives. This advertising does not constitute collection, analysis, or processing of individual user data to target advertising. The information used for targeting is based on the content of the publication, not the individual users, and is generally applicable to the readership rather than to the individual users.

4. Where an online search provider accepts user input for a search query, serves relevant content, and serves advertisements immediately adjacent to that content—for example a search for kayaking supplies and serving ads for paddles—there would generally be no violation. The online search provider constitutes an internet information services provider. Such collection of user search data and processing places this activity in the scope of the conduct regulated by the rule. However, because the data is collected and processed based on the content that a user requested, it is not covered in the definition of individual user data. This activity would not constitute prohibited targeting of advertisement based on individual user data and thus would not violate the rule. In this process, data could not be collected or used as individual user data or else it would be subject to this rule and its processing prohibited.

5. For a data broker that acts as a clearing house for individual user data such as geolocation data, the buying of app-collected or website-collected information would generally be a violation. The data broker constitutes an internet information services provider, and the aggregating of purchased individual user data constitutes processing. Insofar as a data broker collects individual user data to sell to advertisers that individually target users, the practice is in violation of the rule. For example, when a data broker purchases millions of individuals location data from a weather app or Find My Friends and then sells it to advertisers for the purpose of either determining or specifically targeting the recipients, they are in violation of the rule.

6. A data broker that sells aggregated individual user data to advertisers to determine or specifically target ad recipients violates the rule. The data broker constitutes an internet information services provider. The data broker may not have initially collected or even analyzed individual user data. However, aggregation and reselling of such individual user data to other businesses in the advertising market for the purpose of targeting advertising to individuals based on this data constitutes sharing in violation of the rule.

7. A social media site that collects information about the browsing habits of individual users while they are off site, through code embedded on other third-party sites, to retarget advertising to those users violates the rule. A social media site is an internet information services provider covered by the scope of the rule. The mechanism of individual user data collection, through code embedded in other third-party sites, still constitutes individual user data collection by the social media site

even though it is other sites deploying the code. Because this data is then used to automatically target advertisements based on individual user data such as browsing habits, this practice violates the rule.

8. A web browser that creates temporary group profiles based on browsing habits of individual users for the purpose of directing advertisements to those users violates the rule. A web browser constitutes an internet information services provider. The browser's activity is within the scope of the rule because it collects individual user data such as browsing habits and processes those habits into larger group profiles based on this individual user data. While this data may no longer be attached to other personally identifying information, the individual user data is processed and used for targeting advertisements. The source for this targeting is not based on non-user-specific data and thus falls within the scope of the rule. When this data is then distributed for the purposes of algorithmically targeting advertising and marketing to these users such a protocol violates the rule.

9. A social media platform that tracks users' previous clicks to better target ads feeds violates the rule. A social media site is an internet information services provider covered by the scope of the rule. Collecting individual user data places this activity in the scope of the conduct regulated by the rule. Because the social media platform uses individual user data—such as click data—to target advertisements or marketing content, this practice violates the rule.

10. A recruiter collecting information from online sources, like professional networking platforms, to automatically or algorithmically build a relevant mailing

list is in violation of the rule. A mailing list with emails attached to other personally identifying information like names may be considered a collection of individual user data. The information used to build the mailing list would constitute collection of user data for the purpose of online advertising and marketing, and therefore is in violation of the rule. If the only user data collected were the email addresses for the mailing list, and this data were not automatically or algorithmically processed with any other user data, this would fall under the email exemption and thus would not violate the rule.

11. Supermarkets sending out coupons to customers targeted to a recognized place is not a violation of the rule. Supermarkets would fall under the definition of internet information service provider if they engaged in commerce or disseminated information online. The supermarket's collection and processing of customer data, such as purchasing history, would constitute collection of individual user data for the purpose of online advertising and marketing. But because the targeted coupons would be based solely on non-algorithmically selected customer data, it is not a violation of the rule. Targeting customers based on recognized place is exempted.

12. Communications sent out online for volunteering on a political campaign do not violate the rule. The campaign's online communication would fall under the definition of internet information service provider. However, the call for volunteers is not online advertising or marketing because it is an action that does not "commercially benefit" the advertiser and therefore does not violate the rule.

13. In the case of a loyalty program where customers sign up for discounts or product updates from a home goods vendor, using said membership programs for general advertising does not violate the rule. The store would constitute internet information services and advertisements would be sent to the group of customers included in the program. However, the advertisements are directed without regard to the individual user data of those who signed up for the program. Instead, advertisements are directed based on the nature of the loyalty program and the business providing it. This advertising does not constitute collection, use, sharing, or processing of individual user data to target advertising. The information used for targeting is based on the content, not the individual users, and is generally applicable to the subject of the loyalty program rather than to the individual user. Thus, the home goods vendor may have a loyalty program, and sending advertisements or discounts for cutlery to those members would not be a violation.

14. An online sporting goods vendor may have a loyalty program, and using its members' zip code data to target a subset from Boston to sell Bruins tickets would not be a violation. The business/vendor would constitute an internet information services provider, and online advertisements, or marketing would be sent to a subsection of the group of customers who live in a recognized place included in the program. This advertising or marketing, when using any part of the customer data, constitutes collection, use, sharing, or processing of individual user data to target advertising or marketing. The information used for targeting of a subsection of

customers is based on a recognized place and is exempted. Such targeting is not a violation of the rule.

15. In the case of a business using individual user data for internal business analytics measurement purposes, there is no violation. The business would fall under the definition of internet information service provider if they engaged in commerce or disseminated information online. However, the information used to measure aspects of the business such as customer growth or geographic spread would not constitute collection of user data for the purpose of advertising because the information is not used to advertise and therefore is not in violation of the rule. For example, an online magazine using individual user data to track readership or to understand what types of readers are drawn to their content does not violate the rule. Also, the business can analyze advertising measurement data from contextual ads. So long as an internet information service provider does not use individual user data to algorithmically or automatically target individuals for advertising or marketing, the practice of measurement does not violate the rule.

16. In the case of an e-commerce website requesting opt-in consent to track individual user data to serve targeted advertising and marketing based on that user data, there would be a violation. The e-commerce site constitutes an internet information service provider. The collection and use of individual user data falls within the scope of the prohibition. The data is collected and used for the purpose of algorithmically targeting individuals as recipients of online advertising and marketing. User consent does not eliminate or mitigate the violation of the rule.