

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services)	WC Docket No. 16-106

Comments of Audience Partners, LLC

Gregory Guice, Esq.
Jo-Ellyn Sakowitz Klein, Esq.
Daniel Graver, Esq.
Akin Gump Strauss Hauer & Feld LLP
1333 New Hampshire Ave., NW
Washington, DC 20036
(202) 887-4565

Counsel for Audience Partners, LLC

Table of Contents

I.	Introduction.....	3
A.	Background on Audience Partners.....	4
B.	Description of Audience Partners’ Privacy-by-Design Solution	5
II.	Discussion.....	9
A.	IP Addresses Identify Devices, Not Individuals, and Should Be Excluded from the FCC’s Definition of “PII”	11
B.	The Commission Should Develop Its Multi-Pronged Test for the Use and Disclosure of “Aggregate Customer PI” So It Supports Innovative Privacy-by-Design Models and Is Consistent With Congress’ Intent.....	13
1.	The First Prong of the Multi-Factor Approach to Aggregate Customer Information Should Cover <i>Individuals</i> —not <i>Devices</i> — and Should Recognize That an IP Address Is Not Reasonably Linkable to a “Specific Individual”	14
a.	Devices Do Not Have Privacy Rights; People Do.	14
b.	A Data Set Comprised Solely of Aggregated IP Addresses Is Not “Reasonably Linkable” to a Specific Individual.	15
2.	The Second Prong, Related to Public Privacy Commitments, Should Be Satisfied Through Company Privacy Policies.....	17
3.	The Third and Fourth Prongs, Related to Flow-Down Limits on Re-Identification and Downstream Monitoring Requirements, Should Be Appropriately Scaled.....	18
C.	The Commission Should Retain the Plain Meaning and Reasonable Application of the Term “Aggregate Customer Information” as Defined in Sections 222(c)(3) and 222(h)	19
III.	Conclusion	20

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)
)
Protecting the Privacy of Customers of) **WC Docket No. 16-106**
Broadband and Other Telecommunications)
Services)

Comments of Audience Partners, LLC

I. INTRODUCTION

Audience Partners, by its attorneys, submits these comments in response to the Federal Communications Commission’s (“Commission”) Notice of Proposed Rulemaking (“NPRM”) in the above-referenced proceeding, which proposes to impose additional privacy requirements on Broadband Internet Access Service (“BIAS”) providers pursuant to the Communications Act.¹ Audience Partners submits these comments primarily in response to the proposal in the NPRM related to the important statutory carve-out for “aggregate customer information”—i.e., “collective data that relates to a group or category of . . . customers, from which individual customer identities and characteristics have been removed”²—under Section 222(c)(3).³ Audience Partners will demonstrate that aggregate customer information, including data sets comprised of IP addresses, can be used in a way that is highly protective of the consumer’s identity and allows the economic model of an ad-supported Internet to flourish.

¹ *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, FCC 16-39 (rel. Apr. 1, 2016) (*BIAS Privacy NPRM*).

² 47 U.S.C. §§ 222(h)(3).

³ 47 U.S.C. §§ 222(c)(3), (h)(2) (expressly permitting telecommunications carriers to “use, disclose, or permit access to aggregate customer information” without restriction). *See BIAS Privacy NPRM* at paras. 74, 154-166 (emphasis added).

Audience Partners urges the Commission to adopt the proposed rule 64.7002(g) as drafted in Appendix A of the NPRM (“Appendix A”), with slight modifications as noted below. Audience Partners’ privacy-by-design approach is an example of a model tailored to fit within the statutory exception for disclosure of aggregate customer information. The implementation of a regulatory framework, including the multi-factor test the Commission has proposed to determine when aggregate customer personal information may be used, disclosed or accessed, should be narrowly tailored to support innovative privacy models.

A. Background on Audience Partners

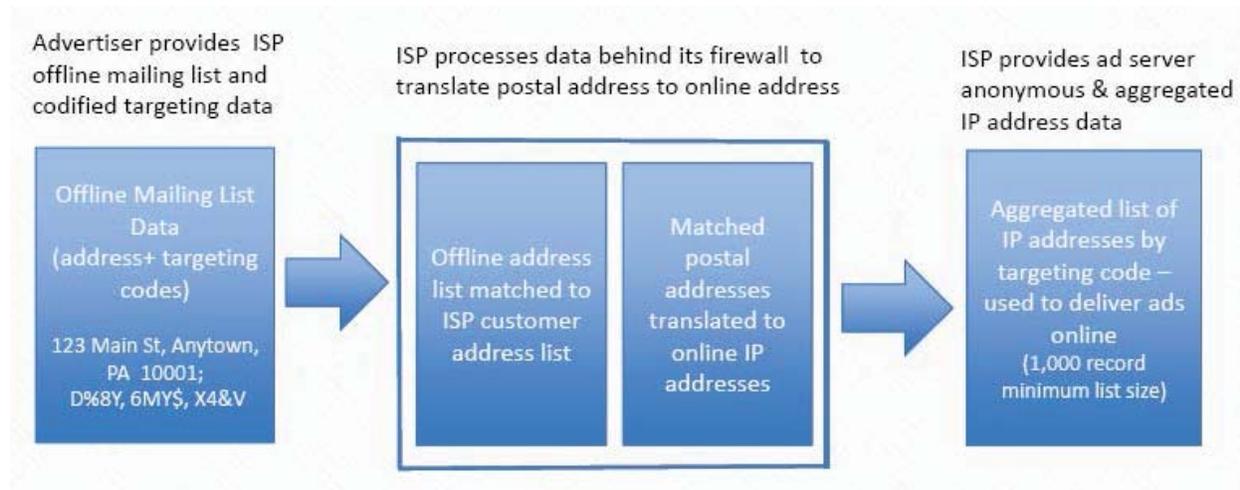
Founded in 2008, Audience Partners has developed a unique advertising platform in cooperation with BIAS providers to allow advertisers to serve addressable ads while maintaining individual privacy. Committed to the principles of privacy-by-design, Audience Partners developed an innovative solution that uses a proprietary, doubleblind privacy® process that completely segregates advertisers and ad servers from individually identifiable information of targeted consumers. This process does not use, collect, or share behavioral data at all—it simply routes ads to the desired destinations while at the same time safeguarding consumer privacy. True personally identifiable information never leaves the BIAS provider’s network; only a routing table of aggregated IP addresses that is not linked to specific individuals is shared with Audience Partners. Ad servers receive no information about any individuals; rather, ads are served to audience segments that are represented by data sets comprised solely of aggregated IP address information.

The only information shared by the BIAS providers with Audience Partners or with ad servers is a routing table of aggregated IP addresses, and those IP addresses are not linked to any information that could be used to identify or re-identify any specific individual. Indeed, routing

tables and IP address information are routinely shared among BIAS providers and ad servers to enable the normal functioning of the Internet, and ad servers already receive IP addresses from consumer devices as part of routine Internet functionality.

B. Description of Audience Partners’ Privacy-by-Design Solution

Audience Partners’ platform uses a proprietary, doubleblind privacy® technique that masks the target audience request using a random code, strips out consumer-specific information, and creates aggregated sets of IP addresses linked to specific target audience segments but not linked to any specific individuals. The system essentially creates a routing table that is simply a subset of the routing tables routinely generated to support Internet traffic. The diagram below illustrates Audience Partners’ unique process for addressable digital advertising:



Audience Partners’ model mimics a direct mail campaign run through a post office. As with any advertising campaign, the process begins with the advertiser identifying a specific audience for its ads, including the traditional direct marketing process of acquiring the physical address of each of the individuals whom the advertiser would like to serve an ad. For example, an advertiser could compile a list of household addresses it believes make up an audience of “Likely Dog Owners,” and send that list to Audience Partners, along with the advertisers’

targeting code for the group (e.g., “LDO1”). Audience Partners masks this information by replacing the advertiser’s targeting code with a new random code (e.g., “Address List X”), just in case the advertiser’s targeting code actually describes the characteristics of the audience. The characteristics of the individuals on this list are as irrelevant to Audience Partners’ model as they would be to the post office—they do not need to know why mail is being sent to an individual, they just need an address so they can route it to the right household.

Audience Partners sends this masked address list to a piece of equipment (the “compiler”) that is owned and operated by the BIAS provider, located within the BIAS provider’s network, behind the BIAS provider’s firewall. The BIAS provider already has both the physical addresses of its customers as well as their current IP addresses (as the BIAS provider is the actual owner of all IP addresses on its network), so they are not collecting any new information. Since the address list is identified solely by a random code, the BIAS provider does not receive any new information about the target audience as part of the process. Moreover, neither the compiler nor Audience Partners has any visibility into the BIAS provider’s “active network path” (i.e., traffic or packets flowing through routers), and therefore neither the compiler nor Audience Partners has any access to customer behavioral data.

The compiler receives “Address List X” and matches it against the BIAS provider’s customer list. The compiler then generates a list of IP addresses that corresponds to the list of matched customers—but that does not include the household addresses—and returns the aggregated list of IP addresses to Audience Partners so it can be used to serve ads associated with the random code.⁴ Audience Partners never has direct access to the BIAS provider’s systems.

⁴ The IP address information is the current IP address information at the time of the ad campaign query. As the IP address information moves forward through Audience Partners’ platform and to the ad server, no other information is attached to the IP address (such as timestamp information) that could be used to identify or re-identify a particular household.

These aggregate IP address lists generated by the compiler are not linked to physical addresses or to any other individually identifiable information.⁵

Further, to ensure there is not a “group of one” or other small sample size, Audience Partners’ solution applies a minimum-match threshold to ensure that any list of aggregated IP addresses is sufficiently large to assure anonymity. At this point, “Address List X” has been converted into an aggregate list of IP address information similar to a routing table. This aggregate list of IP addresses, “IP List X” is re-associated with the advertiser’s original targeting code, so it can be linked to the appropriate advertisement, but it is not linked to any individually identifiable consumer information.

When an individual accesses a website, the website (independent of the BIAS provider) instructs the user’s device to query an ad server to determine what ad content to serve that user (and therefore it is the user’s device that is providing the ad server with its IP address (and cookie identifier) in the first instance, not Audience Partners). The current IP address provided by the device is used by the ad server to determine whether the IP address matches any audience segments. This is done by the ad server querying the routing tables to which it has access. If the IP address is found in a routing table, the appropriate audience segment(s) can be used by the ad server to determine whether or not to serve a particular ad. Neither Audience Partners nor the ad server is able to identify the individual user or their physical address through this query process.

⁵ This privacy-protective process is analogous, in some ways, to the manner in which the front desk of a hotel connects an outside caller with a hotel guest. If you want to reach someone who is checked into a hotel, you can call the hotel operator and ask to speak to hotel guest John Doe, for example. The hotel operator would connect you to John Doe’s room, but would not provide you with his room number or direct dial phone number. Similarly, through the Audience Partners process, ads (like the phone call to the hotel guest) are routed to IP addresses (like the guest’s room), but no information about any individual person (such as the guest’s room number or direct dial phone number) is shared with Audience Partners or the Ad Server. All that is happening through Audience Partners’ process is that an IP address is being identified as being on an aggregated list associated with a particular target audience. No consumer online behavior is tracked, and no geolocation data is collected or used as part of the Audience Partners process. Audience Partners, working in cooperation with BIAS providers, is merely acting like a hotel phone operator or the post office—delivering ads to selected groups of recipients.

All of the steps by and between the user’s device and the ad server are completed with no action or visibility by Audience Partners or its platform.

This unique process allows advertisers to target ads at an addressable level to an aggregate list of households, while assuring individual online privacy through the use of aggregate lists of IP addresses. Through this doubleblind privacy® process, neither the advertiser, nor Audience Partners, nor the ad server gains access to any individually identifiable consumer information, nor does the BIAS provider receive any information about the advertiser, the proposed advertising campaign, or the audience segment being targeted. In the end, this process yields an aggregate, collective data set of IP addresses related to an audience segment from which all individual customer identities and characteristics have been removed.

Audience Partners’ platform and doubleblind privacy® technique have received accolades from the former Information and Privacy Commissioner of Ontario, whose charge included conducting research into privacy issues relating to emerging technologies.⁶ Audience Partners’ unique, doubleblind privacy® platform is also consistent with the privacy-by-design principles advanced by the Federal Trade Commission (“FTC”), as consumer privacy concerns are evaluated and addressed at every point in the process.⁷ Ads are served based on an aggregated compilation of IP address information that is current only at the precise time of the query—just like a routing table—and none of the IP addresses are linked to any individually identifiable consumer information.

⁶ *Redesigning IP Geolocation: Privacy by Design and Online Targeted Advertising*, Information and Privacy Commissioner, Ontario, Canada, available at <https://www.ipc.on.ca/images/Resources/pbd-ip-geo.pdf> (October 2010) (acknowledging the work of Audience Partners’ Bering Media division, to “bake-in privacy from the outset, and fully embrace the concept of Privacy by Design”).

⁷ *See Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FTC Report, Federal Trade Commission, available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> (Mar. 2012) (*hereinafter* FTC Report).

In this fashion, we can use aggregate lists of IP addresses to maximize commercial value and consumer privacy. As evidenced by Audience Partners' privacy-by-design process, the blanket inclusion of IP addresses in the definition of PII is inappropriate, and may in fact be detrimental to consumer privacy. IP addresses on their own are not individually identifiable information. This is especially true given the dynamic nature of most consumer IP addresses (e.g., BIAS providers will re-assign IP addresses based on events as mundane as a consumer unplugging her router). An IP address must normally be linked to other information that is personally identifiable at the time of the initial query to implicate consumer privacy. As is set forth in greater detail below, we believe the final rule should be carefully drafted to assure that we can continue to innovate, build, and utilize systems that maximize commercial value, consumer utility, and consumer privacy.

II. DISCUSSION

Audience Partners is providing these comments to urge the FCC to interpret its statutory authority in a manner that ensures that Audience Partners' carefully balanced, privacy-sensitive model remains viable. It is possible to maintain a commercially viable practice of providing highly targeted ads while protecting individual privacy, but the Commission must be careful to avoid drafting regulations that are so broad that they have unintended and negative consequences for consumer privacy.

First, the Commission seeks comment on the types of data that should be deemed personally identifiable information ("PII") and has proposed to define PII very broadly.⁸ IP addresses identify devices (generally routers), not individuals, and should not be included in any list of protected PII. Further, the use and disclosure of IP addresses is necessary for the basic

⁸ *BIAS Privacy NPRM* at paras. 60–62.

operation of the Internet. Our model provides an example of how using IP addresses can protect consumer privacy. The Commission should avoid drafting a rule that would hinder innovative privacy-by-design models that protect consumer privacy, while allowing traditional advertising models—which collect and use significantly more consumer information, but are not regulated by the FCC—to flourish.

Second, the Commission seeks comment on a proposal to allow BIAS providers to use, disclose, and permit access to aggregate customer PI, without customer approval, for purposes beyond the provision of telecommunications service, “if the provider (1) determines that the aggregate customer PI is not reasonably linkable to a specific individual *or device*; (2) publicly commits to maintain and use the aggregate data in a non-individually identifiable fashion and to not attempt to re-identify the data; (3) contractually prohibits any entity to which it discloses or permits access to the aggregate data from attempting to re-identify the data; and (4) exercises reasonable monitoring to ensure those contracts are not violated.”⁹

Audience Partners generally agrees with the multi-factor approach put forward by the Commission allowing BIAS providers to use, disclose, and permit access to aggregate customer information. Such an approach, however, must be developed carefully to avoid the unintended consequence of hindering activity that protects privacy while enabling commerce, which as the Commission recognizes, is an important objective of this NPRM.¹⁰ For example, in its discussion of the First Prong, the Commission proposed including individuals *and* devices. The statute, however, only references individuals, *not* devices. Devices do not have privacy rights—people do. The Commission should retain Congress’ intent and limit the First Prong of the multi-factor approach to information about individuals, and exclude the reference to devices.

⁹ *Id.* at para. 154 (emphasis added).

¹⁰ *Id.* at paras. 12, 155.

Furthermore, the Commission should recognize that a data set comprised solely of aggregate IP addresses is not “reasonably linkable” to an individual.

Third and finally, as part of this proposal, the Commission also seeks comment on how de-identified, but non-collective data should be treated under Section 222 and its rules. The Commission should retain the plain meaning and reasonable application of the term “aggregate customer information” as defined in Section 222(c)(3) and Section 222(h).

Audience Partners’ privacy-by-design approach is an example of a commercial framework that was specifically tailored to protect consumer privacy and meet the statutory exception for disclosure of aggregate consumer information. The Commission should be careful not to draft a rule that substantially narrows the statutory exception.

As detailed below, we suggest modifications and clarifications to the rule that are needed to ensure that the approach ultimately adopted by the Commission achieves the important objective of protecting privacy while promoting commerce.

A. IP Addresses Identify Devices, Not Individuals, and Should Be Excluded from the FCC’s Definition of “PII”

It is inappropriate and potentially detrimental to individual privacy rights to develop a bright line rule designating IP addresses as PII. IP address blocks and individual device IP addresses are necessarily collected and used for the basic functioning of the Internet. Unlike a Social Security Number, mother’s maiden name, or even an account user name, the IP address identifies a device (generally a router)—not the individual—and is essential to the functioning of the Internet. In the NPRM, the Commission proposes to “provide illustrative, non-exhaustive guidance regarding the types of data that are PII.”¹¹ The NPRM goes on to list a number of elements that would be considered PII, including name, Social Security Number, date and place

¹¹ *Id.* at para. 62.

of birth, etc. In all, the Commission suggests the non-exhaustive PII list include 31 categories of information. While the merits of each is, arguably, worthy of consideration, Audience Partners would like to address why it is inappropriate to include IP address information on this list.

IP addresses are incapable of identifying an individual without being linked to additional information. This is particularly true of dynamic IP addresses. The National Institute of Standards and Technology (“NIST”) guidance on PII, which the NPRM cites as a source that informed the Commission’s thinking, makes this point as well, noting in an example that “[t]he user’s IP address . . . [b]y itself, [is not] directly identifiable data.”¹² The NIST guidance includes as PII only “asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other *host-specific persistent static identifier that consistently links to a particular person* or small, well-defined group of people.”¹³ Even a static IP address, without being linked to other information, does not identify an individual.

The other cases cited by the Commission as a basis for inclusion of IP address in the list similarly include—at most—only “static” or “persistent” identifiers.¹⁴ Audience Partners believes that IP addresses, unless linked to other specifically identifiable personal information, are not PII. The list the Commission has proposed would define all of the other elements that

¹² See National Institute of Standards and Technology (NIST), Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) at § 3.3.2 (2010), http://www.nist.gov/customcf/get_pdf.cfm?pub_id=904990.

¹³ NIST, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology at § 2.2 (2010), http://www.nist.gov/customcf/get_pdf.cfm?pub_id=904990.

¹⁴ See, e.g., *In re Henry Schein Practice Solutions, Inc.*, Agreement Containing Consent Order, F.T.C. File No. 142-3161, at 3 (2016), <https://www.ftc.gov/enforcement/cases-proceedings/142-3161/henry-schein-practice-solutions-inc-matter> (does not include IP address in “personal information”); *In re Credit Karma, Inc.*, Decision and Order, F.T.C. File No. 132-3091, at 2 (2014), <https://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc> (including “static IP address” in “covered information”); Google Inc., Decision and Order, F.T.C. File No. 102-3136, at 3 (2011), <https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter> (including “persistent IP address” in “covered information”); see also Twitter Inc., Decision and Order, F.T.C. File No. 92-3093, at 2 (2011), <https://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation> (including “IP or other persistent identifier” in “non-public consumer information”).

might be linked to an IP address to make it identifiable. If those other elements are removed, the IP address is not identifiable. IP addresses do not need to be included in any list of identifiers that make up PII.

Therefore, we urge the Commission to exclude IP address from any list of types of data that are PII, and clarify that an IP address alone is not deemed linkable to an individual for the purposes of this rule. In the alternative, while it would increase the administrative burden for likely little benefit—and may not in fact be reasonably feasible in all cases—at the very least the Commission should narrow its IP address formulation to focus exclusively on static, unique, and persistent IP addresses.

B. The Commission Should Develop Its Multi-Pronged Test for the Use and Disclosure of “Aggregate Customer PI” So It Supports Innovative Privacy-by-Design Models and Is Consistent With Congress’ Intent

In response to the Commission’s request for comments, set forth below is a prong-by-prong analysis of the test proposed for determining whether BIAS providers may use, disclose, or provide access to aggregate customer information without customer approval. Congress has specified that “a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information” for purposes beyond those required by law and without customer approval.¹⁵ Congress further specified that “[t]he term ‘aggregate customer information’ means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.”¹⁶ The four-pronged test proposed by the Commission should be fine-tuned to remain true to this statutory language and to achieve the proper balance between privacy and commerce.

¹⁵ 47 U.S.C. § 222(c)(3).

¹⁶ 47 U.S.C. § 222(h)(2).

1. The First Prong of the Multi-Factor Approach to Aggregate Customer Information Should Cover *Individuals*—not *Devices*—and Should Recognize That an IP Address Is Not Reasonably Linkable to a “Specific Individual”

The First Prong of the multi-factor approach to determining whether a BIAS provider may use, disclose, or permit access to aggregate customer PI presents two discrete issues on which Audience Partners would like to comment. First, it should not matter whether aggregate customer PI is linkable to a specific device, as the statute only references individual customers (not devices). This standard should be based on whether data is linkable to an individual, not to a device. Accordingly, the Commission should adopt the language set forth in Appendix A, which references only the “specific individual” and not devices. Second, the meaning of “reasonably linkable” should not be construed in an overbroad manner.

a. Devices Do Not Have Privacy Rights; People Do. In the First Prong of the standard as articulated in Appendix A, the Commission states that the BIAS provider must determine “that the aggregate customer PI is not reasonably linkable to a specific individual” to allow for use, disclosure, and access without seeking customer approval.¹⁷ The explanatory text of the NPRM states that the BIAS provider must determine that the customer PI is not reasonably linkable to “a specific individual *or device*,” which is inconsistent with the proposed rule as drafted in Appendix A.¹⁸ Audience Partners urges the Commission to clarify that “devices” are outside the scope of this requirement.¹⁹ Conflating identification of specific individuals with devices and treating them the same is unnecessary to protect privacy concerns for individuals.

¹⁷ *BIAS Privacy NPRM* at App. A, Section 64.7002(g)(1).

¹⁸ *BIAS Privacy NPRM* at para. 154.

¹⁹ *Exportal Ltda v. United States*, 902 F.2d 45, 50 (D.C. Cir. 1990) (“It is well established that a reviewing court owes deference to an agency’s construction of its own regulations. But it is equally well established that this deference is due “only when the plain meaning of the rule itself is doubtful or ambiguous.... Deference to agency interpretations is not in order if the rule’s meaning is clear on its face.” (citations omitted)).

To the extent that the notion that this prong should be extended to devices was drawn from the FTC Report, we urge the Commission to stay true to its own express statute and not be influenced unduly by other regulators operating under more generalized authority. Unlike the FTC, which draws its authority from the broad prohibition against unfair and deceptive acts and practices under Section 5 of the FTC Act, Congress provided the Commission with an express statutory definition for “aggregate customer information” that establishes “*individual* customer identities and characteristics” as the scope of what it is to consider.²⁰ Accordingly, a device should not be considered a “characteristic” of an individual customer’s identity.²¹

For these reasons, Audience Partners urges the Commission to ensure that its final rule and accompanying text clarify that the multi-pronged proposal is focused on ensuring that the aggregated customer PI is not linkable to a specific *individual*.

b. A Data Set Comprised Solely of Aggregated IP Addresses Is Not “Reasonably Linkable” to a Specific Individual. An aggregated list of IP addresses is not “reasonably linkable” to specific individuals. In the NPRM, the Commission seeks comment on ways to ensure that data is not reasonably linkable to specific individuals.²² The Commission asks commenters to “ground their comments in practical examples.”²³

Above, Audience Partners detailed how its product uses aggregated IP addresses, minimum match thresholds, and a doubleblind privacy® technique to ensure that the identity of

²⁰ 47 U.S.C. § 222(h)(3).

²¹ In the context of the Video Privacy Protection Act of 1988, a number of courts have indeed found that device information alone is insufficient for determining an individual’s identity. *See, e.g., In re Hulu Privacy Litigation*, 2014 WL 1724344 (N.D. Cal. Apr. 28, 2014); *In re Nickelodeon Consumer Privacy Litigation*, 2014 WL 3012873 (D.N.J. July 2, 2014); *Eichenberger v. ESPN, Inc.*, C-14-463 TSZ (W.D. Wash. May 7, 2015). *Cf. Yershov v. Gannett Sat. Info. Network, Inc.*, 104 F. Supp.3d 135 (D. Mass. May 15, 2015).

²² *BIAS Privacy NPRM* at para. 157.

²³ *Id.* at para. 156.

specific individuals is not revealed.²⁴ We also noted that IP address information alone is not sufficient to link back to a specific individual for a number of reasons, including the dynamic nature of most consumer IP addresses, whereby the IP address for a particular consumer will change over time.²⁵ Even with IP address and “timestamp” information, which would help determine the window during which the IP address was in use, the information would not be sufficient to identify a specific individual. Audience Partners’ model offers a practical example of an available method and use of technology that allows ads to be served with precision, while only linking to an aggregate table of customer IP addresses, thereby protecting individual privacy. Drafting overbroad limitations on the use of IP addresses would be counter-productive for individual privacy in this case.

The Commission seeks comment on whether it should consider alternative approaches for determining that “individual customer identities and characteristics have been removed,” as provided in Section 222, and looks to HIPAA for potential inspiration. The Commission seeks comment on whether to follow an approach similar to HIPAA’s safe harbor de-identification method, under which a data set may be deemed de-identified and outside the scope of HIPAA’s restrictions if 18 identifiers are removed from the data set and the entity lacks actual knowledge that the information could be used alone or in combination with other information to identify an individual.²⁶

Audience Partners cautions against the use of HIPAA-like standards in this context. Use of the HIPAA safe harbor de-identification standard seems misplaced in this commercial context

²⁴ Audience Partners does not believe that IP address information should be included as personally-identifiable information (PII).

²⁵ See e.g., *Dynamic IP vs Static IP*, <http://whatismyipaddress.com/dynamic-static> (“The biggest advantages of Dynamic IP Addressing are less security risk as the computer is assigned a new IP address each time the customer logs on, they are cost effective and there is automatic network configuration.”).

²⁶ *BIAS Privacy NPRM* at paras. 158, 163.

and should not be applied to data that is not inherently sensitive. If such an approach is pursued, it should be one of many options. Even in the health context, where information is inherently sensitive, HIPAA provides two mechanisms for de-identification—safe harbor is one, and the statistical approach, under which a qualified statistician determines that the data set is de-identified, is a second option. If the FCC decides to follow HIPAA’s lead, at a minimum, both of these options for a de-identification safe harbor and a statistical method should be made available.²⁷

Finally, Audience Partners would note that in the context of the FTC Report much concern was raised about the use of a “reasonable linkability” standard.²⁸ To allay those concerns, the FTC clarified that “as long as (1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company requires downstream users of the data to keep it in its de-identified form, that data will fall outside the scope of the framework.”²⁹ To the extent the Commission chooses to keep the “reasonable linkability” standard as part of the multi-factor approach, Audience Partners supports the adoption of this FTC framework, as it will allow BIAS providers to reasonably determine how to apply this standard to their business practices.

2. The Second Prong, Related to Public Privacy Commitments, Should Be Satisfied Through Company Privacy Policies

The Second Prong would require that the BIAS provider publicly commit to maintaining and using aggregate customer information in a non-individually identifiable fashion and to not attempt to re-identify the data.³⁰ The Commission seeks comment on what action by the BIAS

²⁷ See 45 C.F.R. § 164.514(a)–(c).

²⁸ *FTC Privacy Report* at 21–22.

²⁹ *Id.* at 22.

³⁰ *BIAS Privacy NPRM* at para. 160; App. A, Section 64.7002(g)(2).

provider would satisfy the requirement, asking whether a statement in a BIAS provider’s privacy policy would be sufficient. Audience Partners believes that requiring inclusion of this commitment in a privacy policy is sufficient. As the *FTC Privacy Report* notes, privacy policies “provide an important accountability function.”³¹ Privacy policies have traditionally been viewed by regulators as enforceable commitments to consumers.

3. The Third and Fourth Prongs, Related to Flow-Down Limits on Re-Identification and Downstream Monitoring Requirements, Should Be Appropriately Scaled

The Third and Fourth Prongs would require each BIAS provider to “[c]ontractually prohibit[] any entity to which it discloses or permits access to the aggregate consumer PI from attempting to re-identify such information” and to “exercise[] reasonable monitoring” to ensure these contractual obligations are not violated.³² Audience Partners generally supports the adoption of these prongs, so long as they are reasonably scaled. It is certainly reasonable to flow down contractual obligations not to re-identify information. However, the Commission should offer a mechanism that balances an appropriate level of oversight against the privacy risks and administrative burdens placed on BIAS providers. Notably, not even HIPAA covered entities are required to actively monitor their subcontractors’ compliance with HIPAA, beyond not having actual knowledge the subcontractors are violating HIPAA.³³ This might be an appropriate standard for adoption. For example, if the BIAS provider is simply providing an IP address and nothing else, the Commission might consider adopting under the Fourth Prong a standard that the BIAS provider must have no actual knowledge that the recipient is re-identifying the information

³¹ *FTC Privacy Report* at 61.

³² *BIAS Privacy NPRM* at paras. 161–162; App. A, Section 64.7002(g)(3)-(4).

³³ See 45 C.F.R. § 164.504(e)(2).

in violation of its contractual obligations. Whatever rule the Commission adopts should ensure the administrative cost and burden imposed matches the associated privacy risk.³⁴

C. The Commission Should Retain the Plain Meaning and Reasonable Application of the Term “Aggregate Customer Information” as Defined in Sections 222(c)(3) and 222(h)

The Commission seeks comment on how “de-identified, but non-collective” data should be treated under the rule, noting that aggregate data “by definition must be collective data,” and thereby suggesting that de-identified but non-collective data may fall outside the statutory exception that allows disclosure.³⁵ As defined in the statute, the Commission should recognize that “aggregate information” does not contemplate the exclusion of all individual elements. The statute simply requires the removal of individualized characteristics that, in-and-of-themselves, necessarily identify an individual. This understanding is critical to ensuring that Section 222(c)(3) retains its meaning and purpose.

The Merriam-Webster Dictionary’s definition of aggregate states that “aggregate” is “formed by the collection of units or particulars into a body, mass, or amount.”³⁶ It defines “collective” as “denoting a number of persons or things considered as one group or whole (“flock” is a collective word).”³⁷ Again, the key concept is that individual elements do not lose their identity when placed in a collective or aggregate. Thus, a list of information fitting a set of criteria is “aggregated” information, as it is a collection of individual data presented as a group. Under the statutory definition, “aggregate customer information” means “collective data that relates to a group or category of services or customers” (in Audience Partners’ case, that category

³⁴ See *BIAS Privacy NPRM* at para. 162.

³⁵ *Id.* at para. 165.

³⁶ See <http://www.merriam-webster.com/dictionary/aggregate>.

³⁷ See <http://www.merriam-webster.com/dictionary/collective>.

of customers would be an advertising audience segment).³⁸ From that group, individual customer identities and characteristics must be removed (in Audience Partners' case, this is accomplished by removing everything except the IP address, which, without more, cannot itself be linked to an individual).³⁹ The end result is a de-identified, collective aggregate list of IP addresses (and, notably, IP address blocks are public information).

In determining how to treat de-identified, but non-collective data, Audience Partners urges the Commission to retain the statutory intent and definitions, and confirm that aggregate data, by definition, contemplates the retention of individual elements, which could include an aggregate list of just IP addresses. Moreover, de-identified information is not PII and should not be regulated, regardless of whether it is in the aggregate.

III. CONCLUSION

Audience Partners appreciates the opportunity to provide the Commission an understanding of its business model and how its privacy-by-design platform and doubleblind privacy® technique ensures that consumers do not have to choose between their personal privacy and relevant advertising.

While the Commission has made a number of good suggestions to improve consumer privacy in this NPRM, there are significant changes that should be made in the final rule.

Audience Partners urges the Commission to exclude IP addresses from any list of the types of data that are deemed PII, and to clarify that IP address alone is not deemed linkable to any individual for the purposes of this rule.

Further, Audience Partners urges the Commission to adjust its multi-prong test concerning aggregate customer PI by clarifying that, consistent with the statute, aggregate

³⁸ 47 U.S.C. § 222(h)(2).

³⁹ *Id.*

customer PI should apply to individuals and not devices. Further, under the First Prong, the Commission should clarify that an IP address alone is not reasonably linkable to a specific individual. Under the Second Prong, the Commission should allow notice via the BIAS provider's privacy policies. While the Third Prong's contractual flow-down requirements to prohibit re-identification are reasonable (if properly scoped), the Fourth Prong's downstream monitoring commitments should mirror the current HIPAA monitoring framework, avoid burdensome administration requirements, and require that the BIAS provider not have actual knowledge that downstream companies are violating their contractual requirements not to re-identify individuals.

Finally, the Commission should retain the plain meaning and reasonable application of the term "aggregate customer information," and adopt a policy that de-identified information is not PII, does not pose a significant privacy risk, and should not be regulated (whether or not it is aggregated).

Audience Partners operates like the post office for the Internet, relying on a privacy-by-design model that does not use any behavioral data whatsoever, and hopes that the Commission acts as requested to ensure that this innovative and balanced approach, which was thoughtfully developed to carefully protect consumer privacy while enabling commerce, is clearly preserved.⁴⁰

⁴⁰ Audience Partners maintains business groups that focus on political campaigns and issue advocacy campaigns. Audience Partners also requests that the FCC construe its regulations in a manner to ensure that the opt-in consent requirement does not apply to political speech or nonprofits, consistent with the approach taken under other federal privacy regimes (for example, Do Not Call, Do Not Mail, CAN-SPAM, etc.).