

**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 VERIZON

William H. Johnson
Of Counsel

Karen Zacharia
Catherine M. Hilke
Verizon
1300 I Street, N.W. – Suite 400 West
Washington, D.C. 20005
(202) 515-2438

Scott H. Angstreich
Geoffrey M. Klineberg
Kellogg, Huber, Hansen, Todd,
Evans & Figel, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
(202) 326-7900

Henry Weissmann
Munger Tolles & Olson, LLP
355 South Grand Avenue
35th Floor
Los Angeles, California 90071
(213) 683-9100

Counsel for Verizon

May 27, 2016

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	1
I. THE COMMISSION SHOULD ADOPT A UNIFORM, FLEXIBLE, AND SENSIBLE APPROACH TO NOTICE, CHOICE, AND SECURITY	6
A. Broadband Providers — Including Verizon — Are Committed To Consumer Privacy and Support Consistency	6
B. Consumers Need a Uniform Privacy Regime	7
C. The Commission’s Rules Should Mirror the “Notice-and-Choice” Approach That Applies to All Other Internet Companies	11
D. As an Alternative Approach, the Commission Should Consider Convening a Multi-Stakeholder Process To Develop a Consistent Set of Rules Across the Internet Ecosystem.....	16
E. There Is No Reason To Adopt Special Rules for Broadband Providers.....	16
II. THE COMMISSION’S PROPOSAL DRAWS THE WRONG LINES AND IS UNLAWFUL	24
A. The Proposed Rules for Marketing to Existing Customers Are Bad Policy and Legally Unsupportable.....	24
1. Consumers Will Be Harmed by the Proposed Consent Requirements for Marketing	24
2. The Proposed Consent Requirements for Marketing Are Unlawful	29
B. Restrictions on Broadband Providers’ Ability To Compete in the Digital Advertising Market Are Bad Policy, Anticompetitive, and Legally Unsupportable.....	34
1. Consumers Will Be Harmed by the Opt-In Consent Requirements for Digital Advertising.....	34
2. The Opt-In Consent Requirements for Digital Advertising Are Unlawful	36
3. Prohibitions on “Persistent Identifiers” and “Deep-Packet Inspection” Would Harm Competition	40

4.	Appropriate Use of De-Identified Customer Information Should Not Be Restricted	44
C.	Prohibiting Financial Inducements Is Both Unwise and Unlawful	45
1.	Section 222 Does Not Authorize the Commission To Prohibit Consumers from Receiving Benefits in Exchange for Allowing Use of Their Information	47
2.	Section 201(b) Does Not Authorize the Commission To Prohibit Consumers from Receiving Benefits in Exchange for Allowing Use of Their Information	48
3.	Prohibiting Financial Inducements Violates the First Amendment.....	50
D.	The Statute Provides the Commission with Authority over CPNI, Not All Consumer Data	53
1.	Section 222(a) Only Applies to CPNI	53
2.	No Other Statutory Provision Authorizes the Proposed Rules	60
E.	The Commission Should Allow Business Customers To Negotiate Alternative Arrangements and Customer Information To Be Used To Route Traffic.....	63
1.	The Commission Should Allow Business Customers To Negotiate Specific Privacy Terms	63
2.	As in the Voice Context, Broadband Providers Must Be Allowed To Share Customer Information To Transmit and Route Traffic and for Network Maintenance.....	64
III.	THE INFLEXIBLE DATA-SECURITY AND BREACH-NOTIFICATION PROPOSALS ARE FLAWED AND COUNTERPRODUCTIVE	65
A.	Rigid Data-Security Requirements Would Be Ineffective and Unreasonable.....	65
B.	The Proposed Breach-Notification Requirements Are Inflexible and Burdensome	68
IV.	A PROHIBITION ON ARBITRATION WOULD BE UNLAWFUL AND UNNECESSARY	70
A.	The Commission May Not Restrict Arbitration in Contravention of the Federal Arbitration Act.....	71

B. Prohibiting Arbitration Would Harm Consumers..... 75

CONCLUSION..... 80

APPENDIX (“Summary of Verizon Advertising Programs”)

**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 VERIZON¹

EXECUTIVE SUMMARY

Protecting consumer privacy on the Internet is essential. An effective privacy regime should include the core principles of transparency, customer choice, and data security.

Consumers will benefit most from a privacy regime that applies these principles uniformly to their data regardless of who has it. A consistent regime will avoid creating the consumer confusion, information fatigue, and regulatory uncertainty that would result if consumers are subjected to multiple and varying privacy regimes as they conduct themselves online.

Before the *Open Internet Order*,² all participants in the Internet ecosystem — including the recently reclassified mass-market, retail broadband Internet access service providers — were subject to a uniform system for safeguarding consumer privacy. Indeed, both the Obama Administration, in its Privacy Bill of Rights, and the Federal Trade Commission (“FTC”), in its Privacy Report, noted the importance of having a consistent approach to Internet privacy. Under that existing regime policed by the FTC, the degree of sensitivity of information, not the identity

¹ In addition to Verizon Wireless, the Verizon companies participating in this filing are the regulated, wholly owned subsidiaries of Verizon Communications Inc. (collectively, “Verizon”).

² Report and Order on Remand, Declaratory Ruling, and Order, *Protecting and Promoting the Open Internet*, 30 FCC Rcd 5601 (2015) (“*Open Internet Order*”).

of the entity holding that information, is the touchstone for determining the protections that apply. Opt-in consent — which increases the burdens on both consumers and providers — is reserved for only the most sensitive customer data, such as precise geo-location information, health and financial information, and information associated with children. This existing regime protects sensitive customer information, while at the same time delivering tremendous consumer benefits. Allowing reasonable use of consumer data, while providing consumers with information and choices about the use of their data, enables services that are more affordable for consumers and that are tailored to their needs and interests. This approach also minimizes “notice fatigue” that can lead customers to ignore even important notifications. It has proven to be effective, and the NPRM³ identifies no flaws or failings in that regime.

Verizon has adopted policies designed to implement these core principles throughout its businesses. Verizon explains to its customers how their information may be used, empowers them to make informed choices about the use of their information, and protects its customers’ information using robust security measures. In the event of a data breach, Verizon provides its customers with appropriate notice, which might include information about preventive measures they could take. In other words, the existing notice-and-choice regime is working, and there is no reason to change it.

Although the NPRM recognizes that transparency, customer choice, and data security are core principles informing any privacy regime, the NPRM draws the lines in the wrong places and proposes rules that single out Internet service providers (“ISPs”) for a unique set of burdensome requirements. In doing so, the NPRM rejects the consistent approach endorsed in recent years by

³ Notice of Proposed Rulemaking, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, FCC 16-39 (FCC rel. Apr. 1, 2016) (“NPRM”).

the Obama Administration and the FTC, and it skips the type of multi-stakeholder process that could prove useful in creating a rational and consistent approach to privacy in this complex and evolving marketplace. If adopted, the Commission's proposed requirements will harm consumers by creating confusion, promoting insecurity, and depriving customers of the benefits of competition. Consumers will have to navigate multiple privacy regimes as they switch during the day from broadband providers the Commission has reclassified to those that remain outside of Title II, and as their data traverses the Internet from their broadband provider to a search engine, social network, or smartphone application. Consumers also will be prevented from learning about products and services they are likely to want to use or purchase, or from receiving advertising and other messaging that is more relevant to their interests. The rules would hamstring ISPs and their affiliates from offering customers additional services, which is something all other companies — including their competitors — are able to do. And the rules would prevent ISPs from bringing increased competition to the marketplace for Internet advertising, harming not only the services and products that rely on that advertising, but also the customers who will no longer be able to benefit from them.

The scope of the proposed rules would compound these problems. The Commission's proposed definition of customer proprietary information is too broad and would lead to absurd results. For example, because names and email addresses are considered customer proprietary information, providers not only would be prohibited from targeting advertising to particular customers, but also would be prohibited from notifying all of their customers that they are offering a deal on handset accessories or a new video streaming service. This type of advertising is a common and expected practice of all businesses and one that telecommunications providers

have been lawfully doing for decades. And to the extent a customer does not wish to receive such advertising, they may opt out by being added to providers' Do Not Solicit lists.

The NPRM's proposals are based on a central but flawed premise: that ISPs have unique and comprehensive access to customer information. They do not. Customers' use of multiple broadband providers and the increasing prevalence of encryption mean that broadband providers have little more (and often much less) access to consumer data than other Internet companies. Search engines, social networking sites, email providers, and mobile operating system providers all have extensive access to customer information. In addition, and contrary to the Commission's assumptions, broadband competition — particularly in the hypercompetitive mobile broadband marketplace — protects consumers, who can and do more easily switch mobile broadband providers than mobile operating systems, email providers, social networks, or search engines.

Even putting aside the harms to consumers and competition, the proposed rules are unlawful. The Commission's line-drawing regarding the form of consent required in various contexts — as well as the limitations on sharing information with affiliates and contractors — violates both the Administrative Procedure Act ("APA") and the First Amendment. The same would be true if the Commission were to restrict ISPs from offering customers benefits, including discounts and loyalty programs, in exchange for providing opt-in consent where that is required. Indeed, that proposal conflicts with the fundamental premise of the NPRM that customers are capable of making informed choices about the uses of their information. Furthermore, the Commission's new assertion of authority to regulate not only customer proprietary network information ("CPNI"), but all potentially personally identifiable customer information broadly defined, violates the plain terms of Section 222 of the Communications Act

of 1934.⁴ As the text of that statute and its legislative history make clear, and as the Commission has long recognized, Section 222 authorizes the Commission to regulate only CPNI. No other provision of the Communications Act authorizes the Commission to go beyond CPNI.

Finally, with respect to data security, any data-breach notification requirement should be limited to when a person, without authorization, has intentionally used, disclosed, or gained access to individually identifiable CPNI in a manner likely to cause consumer harm. In addition to striking the right balance between notification and over-notification, this approach has the added benefit of establishing uniform data-breach notification rules for all participants in the Internet ecosystem, so that customers can rely upon consistent, meaningful disclosures.

* * *

Verizon supports the goal of maintaining a robust and consistent consumer privacy framework for all Internet participants. If the Commission adopts privacy and data-security rules, it should apply the principles of transparency, choice, and security in a way that recognizes that the sensitivity of the customer's data should determine the appropriate level of protection. The Commission's proposed rules would not accomplish this goal and would harm consumers and competition. The Commission should, instead, recalibrate its notice-and-choice framework to protect consumers and avoid those harms.

⁴ 47 U.S.C. § 222.

I. THE COMMISSION SHOULD ADOPT A UNIFORM, FLEXIBLE, AND SENSIBLE APPROACH TO NOTICE, CHOICE, AND SECURITY

Broadband providers are only one part of the large and evolving Internet ecosystem.

Over the last decade, the FTC has successfully regulated privacy and data-security practices of all participants within that ecosystem, including ISPs. Consistent with the recommendations in the Obama Administration’s Privacy Bill of Rights, the FTC applied the same standards to those providers’ practices, as it did to practices of all other Internet ecosystem players, including the other “large platform providers” with access to substantial amounts of consumer data. Verizon’s policies and programs have been designed to, and do, comply with this longstanding notice-and-consent framework.

A. Broadband Providers — Including Verizon — Are Committed To Consumer Privacy and Support Consistency

Verizon’s practices are designed to protect and respect consumers’ privacy and the choices consumers make concerning the use of their data. Verizon informs customers about what information it collects and gives consumers choices about how their data may be used. Verizon has several optional advertising and marketing programs, none of which results in the disclosure of individually identifiable information to advertisers.⁵ Those subscribers who choose to participate in these programs have the benefit of receiving relevant advertising about goods and services they are likely to want or need, while also sometimes receiving other benefits, such as loyalty rewards, from Verizon. Verizon fully complies with the FTC’s longstanding privacy framework regarding the protection and use of customer data.

Other broadband providers have similar practices that are designed to protect their customers’ privacy, and the industry is fully committed to ensuring that consumers’ privacy is

⁵ See “Summary of Verizon Advertising Programs” (“Advertising Appendix”) (attached to these Comments).

protected going forward. Earlier this year, five leading telecommunications and technology associations, representing the broadband providers that serve the vast majority of consumers, released a proposal urging the Commission to do just that.⁶ Consistent with the FTC’s technology-neutral approach that requires the same consumer safeguards regardless of the entity that collects the data,⁷ the proposal ensures consumers will be afforded a consistent level of protection across the Internet, while being flexible enough to meet the demands of a constantly evolving marketplace. It proposes that broadband providers give consumers easy-to-understand choices for non-contextual uses of their data, taking into account the sensitivity of the data and the context in which the data is collected.⁸ And it requires reasonable data-security and breach-notification measures.

B. Consumers Need a Uniform Privacy Regime

Consumers accessing the Internet today may do so through multiple broadband providers — depending on whether they are at home or work, or using their smartphone’s LTE radio or a

⁶ See Letter from the American Cable Association, the Competitive Carriers Association, CTIA[®], the National Cable & Telecommunications Association, and the U.S. Telecom Association to Chairman Tom Wheeler, FCC (Mar. 1, 2016) (“Broadband Providers Letter”), available at <https://www.ustelecom.org/sites/default/files/documents/Wheeler%20Letter%20Re%20Privacy%20Principles%203%201%2016%20%283%29.pdf>.

⁷ See FTC, *FTC Report: Protecting Consumer Privacy in an Era of Rapid Change – Recommendations for Business and Policymakers* 56 (Mar. 2012) (“FTC 2012 Report”), available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>; FTC, *Workshop: The Big Picture – Comprehensive Online Data Collection*, Transcript at 272-74 (Dec. 6, 2012), available at https://www.ftc.gov/sites/default/files/documents/public_events/The%20Big%20Picture%3A%20Comprehensive%20Online%20Data%20Collection/bigpicture_transcript_21206ftc.pdf.

⁸ A non-exhaustive list of examples of “contextual uses” of data include “product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers.” Broadband Providers Letter, Attach. at 3.

WiFi hotspot at coffee shop.⁹ In addition, while broadband providers may transmit consumers' data over their network, that same data (and more) is stored on edge providers' servers and available to operating system providers. Given the myriad entities that have access to consumer data as it travels across the Internet, consumers have a strong interest in having a *uniform* privacy regime apply to each company with access to their data.

Consumers reasonably expect that their personal information will be subject to the same set of rules in all contexts, regardless of how the information is transmitted or where (or by whom) in the cloud it may be stored. If consumers must deal with varying standards for choice and transparency depending on how they access the Internet or what websites they visit, they will inevitably become confused, frustrated, and fatigued with privacy rules and notices. Having a consistent framework — one that treats an individual's data the same regardless of what company possesses it — will prevent these ills. Indeed, achieving consistency is a primary goal of the White House 2012 Privacy Report, which recognizes that “[n]ationally uniform consumer data privacy rules are necessary to create certainty for companies and consistent protections for consumers.”¹⁰ The White House even concluded that, “[b]ecause existing Federal laws treat

⁹ In the *Open Internet Order*, the Commission “decline[d] to apply the open Internet rules to premises operators — such as coffee shops, bookstores, airlines, . . . and other businesses that acquire broadband Internet access service from a broadband provider to enable patrons to access the Internet from their respective establishments.” *Open Internet Order* ¶ 191. Moreover, because the Commission’s reclassification decision includes only providers that sell broadband to “residential customers, small businesses, and other end-user customers such as schools and libraries,” *id.* ¶ 189, in many cases both the premises operator *and* the broadband provider will not be subject to any rules the Commission adopts under Section 222. The Commission’s reclassification decision also does not include broadband service sold to edge providers and enterprise customers. *See id.*

¹⁰ White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* 37 (Feb. 2012) (“White House 2012 Privacy Report”), available at <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf>. As the Electronic Privacy Information Center (“EPIC”) stated in its March 2016 letter to the Commission, the Commission’s “narrow focus on ISPs” is misplaced,

similar technologies within the communications sector differently, the Administration supports simplifying and clarifying the legal landscape and making the FTC responsible for enforcing the Consumer Privacy Bill of Rights against communications providers.”¹¹

By contrast, having to deal with different and even inconsistent privacy frameworks will inevitably lead to consumer confusion and frustration. As the Commission noted, even customers who value privacy may “fail to spend time and energy making multiple, complex privacy choices.”¹² If different rules apply to different participants in the Internet ecosystem, customers would have to learn that, when their information is held by their home or mobile broadband provider, it is subject to one privacy framework with opt-in requirements for some information and uses and opt-out requirements for others. And customers would also have to understand that a wholly different privacy framework with different opt-out and opt-in requirements applies when that very same information is held by the broadband providers at their workplaces, a store owner that operates a WiFi hot spot, an edge provider, or an operating system provider.

This approach is inconsistent with what the White House has described as the “important” objective of “creating a level playing field for companies [and] a consistent set of

because broadband providers are “not the only so-called gatekeepers to the Internet who have extensive and detailed views of consumers’ online activities. Indeed, many of the largest email, search, and social media companies *exceed the scope and data collection activities of the ISPs*. A failure to protect the privacy of consumers from these Internet-based services is a failure to provide meaningful communications privacy protections.” Memorandum from Claire Gartland et al., EPIC, to Interested Persons, *Re: FCC Communications Privacy Rulemaking* at 1 (Mar. 18, 2016) (emphasis added), *available at* <https://epic.org/privacy/consumer/EPIC-Draft-FCC-Privacy-Rules.pdf>.

¹¹ White House 2012 Privacy Report at 39 (footnote omitted)

¹² NPRM ¶ 106 n.186.

expectations for consumers.”¹³ In its proposed framework for protecting privacy and promoting innovation, the White House stressed the importance of maintaining a regime of “[n]ationally uniform consumer data privacy rules” in order “to create certainty for companies and consistent protections for consumers.”¹⁴ The Commission’s proposed rules risk undermining these Administration goals without any countervailing benefit for consumers.

In addition, consumers would naturally (but mistakenly) assume that, if they are required to opt-in for broadband providers to use certain types of information, others with access to the same information also would be required to seek their opt-in consent before using that information for similar purposes. Similarly, consumers would erroneously assume that, when they decline to opt in to their broadband provider’s advertising program, that decision would also apply to the wide range of other Internet companies that use the same data for advertising. This very basic failure contradicts the repeated recognition that a consistent privacy framework for all Internet participants is in the public interest.¹⁵ As the Obama Administration emphasized in its 2012 Privacy Report, there should be a “comprehensive set of privacy protections in the commercial marketplace” that upholds the “important” principles of a “level playing field for companies [and] a consistent set of expectations for consumers.”¹⁶

Moreover, consistency across all players in the Internet ecosystem will promote competition in the marketplace for digital advertising. The Commission’s goal should be to

¹³ White House 2012 Privacy Report at 36.

¹⁴ *Id.* at 37.

¹⁵ See Margaret Harding McGill, *FCC, FTC Chiefs Zero In On Data Security, Privacy*, Law360 (Jan. 6, 2016) (quoting FCC Chairman Tom Wheeler’s remarks at the January 6, 2016 Consumer Technology Association show: “What the FTC has done in that regard is to build a terrific model and so I think one of our challenges is to make sure we’re consistent with the kind of thoughtful, rational approach that the FTC has taken.”), available at <http://www.law360.com/articles/743314/fcc-ftc-chiefs-zero-in-on-data-security-privacy>.

¹⁶ White House 2012 Privacy Report at 36.

encourage competition by providing a level playing field and ensuring that broadband providers — the most likely new entrants into the advertising marketplace — face the same rules as the market leaders. By contrast, imposing more onerous rules on broadband providers would undermine competition.¹⁷

C. The Commission’s Rules Should Mirror the “Notice-and-Choice” Approach That Applies to All Other Internet Companies

Prior to the *Open Internet Order*, consumer data sent over the Internet was subject to a uniform and well-functioning regime administered by the FTC. That same regime will continue to apply to all participants in the Internet ecosystem — including numerous broadband providers — except for the mass-market broadband Internet access service providers whom the Commission has now reclassified. As the Commission acknowledges, the FTC has a “robust privacy enforcement practice” that aims to ensure consumer choice and consumer control over the use of data.¹⁸ Under that framework, companies in the Internet ecosystem must ensure that their privacy and data-security practices are neither unfair nor deceptive to consumers.¹⁹

The FTC has developed privacy policy and enforced privacy laws since the 1970s. In 2012, following a multi-year process in which more than 450 interested parties submitted

¹⁷ The FTC also has warned against “potentially inconsistent privacy obligations.” FTC 2012 Report at 16; *see also* Michael O’Rielly & Maureen K. Ohlhausen, *The Consequences of a Washington Internet Power Grab*, Wall St. J., Aug. 6, 2015 (“[I]mposing new obligations that conflict with what other agencies, particularly the FTC, were already doing will cause companies to spend more time and money on compliance, and less on investing in networks and developing the next breakthrough technology. In the longer term, imposing an outdated common-carrier privacy and security regime on providers will diminish consumers’ Internet experiences.”), *available at* <http://www.wsj.com/articles/the-consequences-of-a-washington-internet-power-grab-1438903157>.

¹⁸ NPRM ¶ 132.

¹⁹ *See* 15 U.S.C. § 45(a) (FTC Act prohibiting “unfair or deceptive acts or practices in or affecting commerce”).

comments and numerous workshops were held,²⁰ it issued a privacy framework intended to articulate best practices for companies that collect and use consumer data. These best practices guide companies as they develop and maintain processes and systems to put in place privacy and data-security practices within their businesses.²¹

This existing framework, which imposes more stringent requirements on sensitive data, reflects a careful, thoughtful balance between privacy and innovation. Notably, this longstanding approach has allowed for explosive growth in Internet and broadband usage and flexibility for evolving business models, while also vigorously protecting privacy rights and punishing unfair or deceptive practices. Where violations and misleading practices have occurred, the FTC has brought dozens of enforcement actions, including many since 2010 relating to misleading practices in the use of consumer data.²²

It is in part because the United States government has taken a pragmatic approach to data use and privacy that the country's digital economy has flourished. U.S. regulators, including the FTC, have long shared with international counterparts how the U.S. privacy framework is one that is balanced — it successfully achieves privacy protection, while at the same time allowing flexibility for innovative new services that often depend on using consumer data. U.S.

²⁰ Prior to release of the preliminary FTC Staff report (*available at* <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf>), the FTC held a series of privacy roundtables. *See* FTC, *Exploring Privacy – A Roundtable Series* (Dec. 7, 2009), *available at* <http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml>. The second and third roundtable events took place on January 28, 2010, and March 17, 2010. *See id.* Following the release of the preliminary report and issuance of the final report, the FTC held forums on child identity theft (<https://www.ftc.gov/news-events/events-calendar/2011/07/stolen-futures-forum-child-identity-theft>) and on the privacy implications of facial recognition technology (<https://www.ftc.gov/news-events/events-calendar/2011/12/face-facts-forum-facial-recognition-technology>).

²¹ *See* FTC 2012 Report at iii.

²² *See id.* at ii.

policymakers have also long urged foreign jurisdictions to avoid prescriptive privacy frameworks that do not allow for this flexibility and innovation. The Commission’s proposed rules, however, would disrupt the balance in the United States. If it adopts its proposed rules, the Commission would dismantle the longstanding and successful approach to privacy, which has focused on matching restrictions to the sensitivity of data. That step would undermine U.S. government efforts to encourage sensible privacy regimes around the globe. It is no understatement to say that this risks a massive disruption to the Internet economy. Much of the commerce on the Internet — from news, to apps, entertainment, email, and search — is made available to consumers for free based on the fundamental exchange of value for the services delivered and the information provided by consumers to support advertising.

To the extent its Title II authority over broadband is upheld, the Commission should adopt rules under Section 222 that are consistent with the FTC’s consent framework, which is attuned to the sensitivity of the data being collected or shared and treats all players in the Internet ecosystem equally. These rules should only apply to individually identifiable CPNI, as that term is defined in Section 222 of the Communications Act,²³ and to circumstances when telecommunications service providers are providing a telecommunications service and receive CPNI solely by virtue of the provider-customer relationship. The Commission’s rules should focus on four core privacy principles: transparency, consumer choice, data security, and data-breach notifications. These are the same core principles that the Commission has embraced in the NPRM,²⁴ but they should be applied in a manner consistent with the standards that apply to all others in the Internet ecosystem.

²³ 47 U.S.C. § 222.

²⁴ See NPRM ¶¶ 9, 23.

- *Transparency.* Telecommunications service providers should provide notice describing the information they collect, how they use it, and for what purposes, if any, they share that information with third parties.

- *Consumer Choice.* Telecommunications service providers should be permitted to use and disclose information in a manner consistent with the context in which the customer provides it. For example, providers should be allowed to use and share customer information for product and service fulfillment, billing and collection, fraud prevention, and emergency response assistance. In addition, choices for first- and third-party marketing should be different.

Customers have come to expect companies with whom they already do business and their affiliates to offer them new products and services. Therefore, consent to use less sensitive customer information (such as an email address, the type of service plan to which the customer subscribes, or the accessories they may have purchased) should be inferred for such first-party marketing. On the other hand, consumers may not always expect providers to offer them third-party products or services, so providers should give customers easy-to-understand choices prior to using data to serve third-party advertisements. Providers should consider the sensitivity of data and the context in which the provider received the information in determining what type of customer choice is appropriate. The FTC views precise geo-location information, health and financial information, Social Security numbers, and information associated with children as “sensitive.”²⁵ Verizon today takes the conservative approach of requiring opt-in consent before using any precise geo-location information or web browsing information to serve third-party ads.²⁶ Finally, broadband providers also should be permitted to share customer information with

²⁵ FTC 2012 Report at 59 (“Accordingly, before collecting such data, companies should first obtain affirmative express consent from consumers.”).

²⁶ See Advertising Appendix at 5-6.

affiliates based on implied consent, provided that the affiliate honors the customer's choices prior to using that data.

- *Data Security.* Telecommunications service providers should establish data-security programs that include physical, technical, and administrative security safeguards to protect customer information from unauthorized access, use, and disclosure that are reasonable in light of the nature and scope of the provider's activities, the sensitivity of the data, and the size and complexity of the provider's data operations.
- *Data-Breach Notifications.* Telecommunications service providers should notify customers whose information has been breached whenever failing to provide such notice could potentially harm the consumer.

Rather than dictating specific and inflexible methods that will quickly become outdated as the market and technology evolve, this framework identifies the privacy and security goals telecommunications providers should follow and provides them flexibility in how to meet them. This goal-specific orientation will enable broadband providers to respond to changes in technology, business models, and consumer expectations while maintaining robust levels of privacy and security. This approach also recognizes that opt-in consent may be appropriate for the most sensitive forms of consumer information. And it ensures that the privacy framework governing broadband providers is consistent with the privacy framework governing all other players in the Internet marketplace.²⁷

²⁷ See generally FTC 2012 Report.

D. As an Alternative Approach, the Commission Should Consider Relying on a Multi-Stakeholder Process To Develop a Consistent Set of Rules Across the Internet Ecosystem

An effective, alternative approach to addressing privacy and data security would be for the Commission to support a multi-stakeholder process to develop an appropriate, consistent, and flexible framework. Such a process could involve all impacted entities, including telecommunications service providers, operating systems, search engines and social networks, other edge providers, consumer groups, diversity groups, advertising networks, associations, privacy advocates, and other government agencies. As the Obama Administration has found, “open, transparent multi-stakeholder processes . . . , when appropriately structured, . . . can provide the flexibility, speed, and decentralization necessary to address Internet policy challenges,” and a “process that is open to a broad range of participants and facilitates their full participation will allow technical experts, companies, advocates, civil and criminal law enforcement representatives responsible for enforcing consumer privacy laws, and academics to work together to find creative solutions to problems.”²⁸ Given the complexity of issues affecting Internet privacy and security, the wide range of interested stakeholders, and the long history of effective self-regulatory initiatives in the context of privacy, a multi-stakeholder approach would be a more effective alternative to traditional, prescriptive regulation. Such a process could ensure appropriate, flexible standards to protect consumers regardless of the companies with which they interact, as technology and business models evolve over time.

E. There Is No Reason To Adopt Special Rules for Broadband Providers

In the NPRM, the Commission proposes to adopt unique rules for broadband providers. But there is no evidence that the existing privacy approach, which has applied to all participants

²⁸ White House 2012 Privacy Report at 23.

in the Internet marketplace, including broadband providers, has come up short in protecting privacy or encouraging broadband deployment or adoption.

The Commission’s proposal to single out ISPs for heightened regulation is based on a faulty premise. The Commission states that broadband Internet service providers, alone among all the participants in the Internet ecosystem, have “highly detailed and comprehensive profiles of their customers” and “are the most important and extensive conduits of consumer information.”²⁹ Accordingly, the Commission concludes that broadband Internet access service providers “have direct access to potentially *all* customer information,” which distinguishes them from edge providers that “only have direct access to the information that customers choose to share with them.”³⁰

But that mischaracterizes the relationship between broadband providers and their customers’ data. Although broadband providers of course have access to considerable consumer data, they do *not* have either a unique or a comprehensive window into that data.³¹ Rather, because of evolving technology and consumer patterns, as a recent report explained, “[a]ny one ISP today is . . . the conduit for only a fraction of a typical user’s online activity.”³²

As compared to broadband providers, other participants in the Internet ecosystem — including social networks, advertising networks, search engines, email services, and operating

²⁹ NPRM ¶¶ 2, 4.

³⁰ *Id.* ¶ 132.

³¹ See Peter Swire, Associate Director, et al., Georgia Tech Inst. for Info. Sec. & Privacy, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* 7 (Feb. 29, 2016) (“*Swire Report*”) (“First, ISP access to user data is not *comprehensive* — technological developments place substantial limits on ISPs’ visibility. Second, ISP access to user data is not *unique* — other companies often have access to more information and a wider range of user information than ISPs.”), available at http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf.

³² *Id.* at 3.

system and device developers — have at least equal, if not better, access to customer information. Americans spend hours every day on social media, checking their social media accounts on average 17 times daily.³³ Those repeated and prolonged interactions provide social networking sites with access to vast amounts of commercially valuable information about their users, including user-generated content and metadata, which they use to facilitate targeted advertising. As social networking sites evolve, these interactions are growing to include access to business pages that can substitute for websites, commercial feeds, and news, video, and entertainment that would previously have been accessed through a company’s app or website.³⁴ Search engines collect data from every search (indeed, every *letter* typed into a search bar, even if the search is abandoned) by many millions of users, which gives search engines “extensive access both to detailed URLs” and to user content that is frequently linked to individual users’ other online activities.³⁵ That data is packaged and sold and “provides advertisers with nuanced insight into each user’s intent.”³⁶ Email providers scan the contents of their users’ email for targeted advertisements and other services.³⁷ Operating systems (including mobile operating systems) have the technical capacity to see “every keystroke entered, word typed, and image

³³ *Id.* at 43.

³⁴ *See, e.g.*, Brittney Helmrigh, *Social Media for Business: 2016 Marketing Guide*, Business News Daily (Jan. 29, 2016) (summarizing business marketing opportunities on prominent social networking sites), *available at* <http://www.businessnewsdaily.com/7832-social-media-for-business.html>; Kathleen Chaykowski, *Number Of Facebook Business Pages Climbs To 50 Million With New Messaging Tools*, Forbes (Dec. 8, 2015), *available at* <http://www.forbes.com/sites/kathleenchaykowski/2015/12/08/facebook-business-pages-climb-to-50-million-with-new-messaging-tools/>.

³⁵ *Swire Report* at 56.

³⁶ *Id.* at 54.

³⁷ *Id.* at 61.

viewed” on a given device.³⁸ Mapping and planning apps provide highly granular insights into consumers’ location, movement throughout the day, stores visited, and personal interests.

Mobile operating systems track their users through an ID that is specifically used and widely shared for advertising.³⁹ It is common for Internet players to connect with customers through many of these means and deterministically link that data to a person through a first-party login.

None of that data collection — nor its use and sale for advertising purposes — would be subject to the Commission’s proposed rules (nor should it be). The same is true of the myriad broadband providers whom the Commission has not reclassified, including those who provide the Internet access that individuals use while at work or at coffee shops or airports, as well as the providers that sell Internet access to edge providers. Because *all* of these participants in the Internet ecosystem have access to users’ information, the Commission in implementing Section 222 is not creating “sector-specific” rules, but instead is adopting rules for a small subset of a much larger sector.

While reclassified broadband providers have access to certain consumer data, that access is not materially different from any of these other providers, nor is it comprehensive or unavoidable by consumers. For example, ISPs have access to information that consumers share with virtually every company with whom they do business online and in the physical world. Included in this category is information like a customer’s name, physical address, email address, telephone numbers, and the services they are purchasing from that company. Nevertheless, the Commission has proposed to require ISPs to secure opt-in consent to use this information as part of their advertising programs even though other companies with access to the very same information face no such restrictions.

³⁸ *Id.* at 67.

³⁹ *Id.* at 68.

Moreover, even with respect to information that is transmitted as part of the Internet service itself, ISPs have limited unique access to that information. Whereas in the 1990s, a typical user interacted with the Internet from a “single, stationary home desktop,” today the average Internet user has 6.1 connected devices, many of which are mobile — including smartphones, tablets, laptop and home computers, and other devices.⁴⁰ These devices are often served by multiple ISPs. For example, a Verizon wireless customer might use Verizon’s broadband Internet access service with her smartphone, but have different ISPs for her home desktop and tablet, to say nothing of the other providers that she uses while at work or on WiFi hotspots. Verizon would have access to only one small slice of that subscriber’s overall Internet use (*i.e.*, unencrypted use on Verizon’s mobile network when not connected to her home, or a public, WiFi network). Indeed, a majority of all mobile data soon will be sent across WiFi networks and not mobile broadband connections like 4G or 5G networks.⁴¹ Verizon and other broadband providers lack visibility into much of that traffic, as a growing number of WiFi networks exist outside the home and are provided by companies that the Commission has not reclassified as common carriers subject to Section 222.⁴² This stands in contrast to many other players in the Internet ecosystem who may interact with users across all of their devices.

In addition, encryption techniques increasingly shield customers’ data, including their IP addresses, from their broadband providers. “Today, all of the top 10 websites either encrypt by default or upon user log-in, as do 42 of the top 50 sites.”⁴³ In particular, the use of HTTPS — which prevents broadband providers from seeing the content and detailed URLs of their

⁴⁰ *Id.* at 7.

⁴¹ By 2014, 46% of mobile data traffic was off-loaded to WiFi networks; that figure will grow to 60% by 2020. *See id.* at 3.

⁴² *See supra* note 9.

⁴³ Swire Report at 3.

customers — is the “new normal.”⁴⁴ HTTPS traffic has risen sharply from 13% to 49% just since April 2014.⁴⁵ It will comprise an estimated 70% of all online traffic by the end of this year.⁴⁶ “Encryption such as HTTPS blocks ISPs from having the ability to see users’ content and detailed URLs. There clearly can be no ‘comprehensive’ ISP visibility into user activity when ISPs are blocked from a growing majority of user activity.”⁴⁷ Furthermore, when consumers choose to use virtual private networks, which are now becoming more readily available,⁴⁸ the broadband provider cannot even see the domain name that a user is visiting, much less the content of the packets being sent and received.

In any event, particularly in the competitive marketplace, consumers can avoid sharing their data with a particular broadband provider by either switching to another provider or relying on services such as WiFi. The same mobile broadband subscriber who could readily choose to switch providers over lunch would likely have to think long and hard before abandoning her current social network, email service, or mobile operating system platform. Social sites are only valuable if all of one’s friends and contacts are also present; email addresses are not portable, and a new one must therefore be shared with all personal and commercial contacts; switching mobile operating systems means switching phones, which can be an expensive and inconvenient proposition for many consumers. This stands in sharp contrast to telephone numbers and mobile

⁴⁴ *Id.* at 35.

⁴⁵ *Id.* at 3.

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ For example, the Opera browser now comes with a built-in, free VPN. *See* Opera, *Free VPN integrated in Opera for better online privacy*, <http://www.opera.com/blogs/desktop/2016/04/free-vpn-integrated-opera-for-windows-mac/> (offering “a free, unlimited, native VPN that just works out-of-the-box and doesn’t require any subscription” to “VPNs available to everyone”) (last visited May 25, 2016).

devices, which are ubiquitously portable. The Commission, however, justifies its regulations in part by asserting that

a consumer, once signed up for a broadband service, simply cannot avoid that network in the same manner as a consumer can instantaneously (and without penalty) switch search engines (including to ones that provide extra privacy protections), surf among competing websites, and select among diverse applications.⁴⁹

Thus, it concludes that “broadband networks are not, in fact, the same as edge providers in all relevant respects.”⁵⁰ This conclusion is wrong.

As an initial matter, the Commission ignores that, when a customer “surf[s] among competing websites” using a single browser or applications on a mobile device, the browser or operating system running on the device can obtain the same information about each of the visits to each of the websites. So the browser and operating system have access to virtually all information regarding the activities of customers while using their devices. And there are advertising networks that use cookies on multiple sites to track customers moving from one website to another.

Moreover, customers can easily switch broadband providers if they are dissatisfied with their privacy policies. With respect to wireless broadband, the reality is that consumers *do* switch providers frequently and with increasing ease. According to the *Eighteenth Mobile Competition Report*, for the year ending with the second quarter of 2015, the top four mobile providers on average lost 21.49% of their subscribers per year.⁵¹ In contrast, over the same

⁴⁹ NPRM ¶ 4.

⁵⁰ *Id.*

⁵¹ Eighteenth Report, *Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993; Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services*, 30 FCC Rcd 14515, ¶ 20 & Chart II.B.6 (2015) (“*Eighteenth Mobile Competition Report*”) (showing an annual 17.5% churn rate for AT&T, 15.6% for Verizon, 27.15% for Sprint, and 26.1% for T-Mobile). Although the

period, only 13.4% of customers buying a new Android powered smartphone switched from an iPhone to Android.⁵² This is, in part, because wireless providers aggressively offer customers financial and other inducements to switch service providers.⁵³ For example, some wireless providers offer month-to-month postpaid contracts (without early termination fees) and prepaid plans. Neither penalizes a customer for switching to a new provider. Even plans with early termination fees often prorate them, which can lower the barrier to switching while still allowing customers to purchase a new device at a substantial discount. Some wireless providers offer to buy customers out of their contracts with other providers. Verizon, for example, offers new customers a financial incentive for an old device to help offset termination fees imposed by other providers. Number portability and the ability to unlock devices also permit customers to switch providers more easily than ever.⁵⁴

In sum, there is no basis for unique rules for one segment of the Internet marketplace.

The FTC's notice-and-choice regime has proven successful, and reclassified broadband Internet

chart purports to show “quarterly” churn, the Report’s text makes clear that the figures provided are in fact the average monthly churn figures for each provider during the quarter at issue. *See id.* ¶ 20.

⁵² *See* Endeavor Partners, *US Smartphone OS Loyalty Survey: Q2 2015* (Sept. 2015), <http://endeavourpartners.net/us-smartphone-os-loyalty-survey-q2-2015/>.

⁵³ *See generally* Comments of Verizon at 31-35, *Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993; Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services*, WT Docket No. 15-125 (FCC filed June 29, 2015); Andres V. Lerner & Janusz A. Ordovery, *The “Terminating Access Monopoly” Theory and the Provision of Broadband Internet Access* 7-8, 12-14 (Jan. 15, 2015) (“Lerner/Ordovery White Paper”), attached to Ex Parte Letter from Kathleen Grillo, Verizon, to Marlene H. Dortch, FCC, GN Docket No. 14-28 (FCC filed Jan. 15, 2015).

⁵⁴ Competition is not limited to wireless providers. Virtually all of Verizon’s Fios subscribers can choose to get Internet through high-speed cable services. *See* Lerner/Ordovery White Paper at 24. Competition between these services is stiff in high-demand areas, leading to significant customer switching among providers. *See id.* at 26-27. In 2014, 17.6% of consumers had switched wireline broadband providers within the last 12 months, and fully one-third had switched in the last two years. *See id.* at 27.

access service providers do not occupy a unique position within the Internet ecosystem.

Consumers, moreover, benefit from a uniform regime that applies to all of the data they send over the Internet.

II. THE COMMISSION’S PROPOSAL DRAWS THE WRONG LINES AND IS UNLAWFUL

The Commission’s privacy proposals with respect to marketing to customers and Internet advertising more generally are both bad policy and unlawful. Rather than focusing on the sensitivity of the information at issue and calibrating protections accordingly, the Commission has made the proposed use of the data and the identity of the holder of the information what matters. This makes no sense with respect either to safeguarding customer privacy or to promoting a competitive market for Internet services and online advertising. It also violates Section 222, the APA, and the First Amendment.

A. The Proposed Rules for Marketing to Existing Customers Are Bad Policy and Legally Unsupportable

1. Consumers Will Be Harmed by the Proposed Consent Requirements for Marketing

Like other companies, broadband providers should be permitted to market their services to their own customers (and to allow their affiliates to do so) without first obtaining opt-in or opt-out consent. Customers already reasonably assume that they have given their implied consent to receive offers from their own provider or from an affiliate of that provider to market any of those companies’ services — not just services to which the customer already subscribes. That is exactly what consumers assume when dealing with all other businesses — both on the Internet and in the brick-and-mortar world. For example, Uber can notify its customers that they might like to download Uber Eats. And a restaurant group can notify its frequent diners of a new restaurant without first obtaining express permission. But, under the proposed rules, broadband

providers would be singled out and *prohibited* from sending an email to any of their customers notifying them that the company has launched a new product or service. This prohibition conflicts directly with how telecommunications carriers have been operating under the Commission’s existing CPNI rules for years, and how the rest of the Internet economy (and the broader U.S. marketplace) will continue to work. Broadband providers should thus be permitted to use customer information to market their own products and services to their customers. Broadband providers should similarly have the ability to share customer information with affiliates without seeking additional approval from customers (opt-out or opt-in).

First, the Commission’s sole apparent justification for imposing these marketing requirements is that the restriction is “consistent with customers’ expectations” because “customers desire and expect the opportunity to affirmatively choose how their information is used.”⁵⁵ But the only authority the Commission cites for its understanding of “customers’ expectations” is a 2016 report by the Pew Research Center that the Commission believes shows that “customers are more comfortable with use of their information when the use is internal and related to marketing the service they are using.”⁵⁶ The report, which appears to rely primarily on anecdotal evidence, does not say that. Rather, the cited portions of the report indicate only that some customers are unhappy when their data is “*shar[ed] . . . with a third party.*”⁵⁷ Indeed, the

⁵⁵ NPRM ¶¶ 123, 127.

⁵⁶ *Id.* ¶ 123 n.210. See also Lee Rainie & Maeve Duggan, *Privacy and Information Sharing* (Pew Research Center Jan. 14, 2016) (“2016 Pew Report”), available at http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf.

⁵⁷ 2016 Pew Report at 24 (emphasis added); see also *id.* (customer expressing preference for being able to “opt out on sharing with third parties”).

report actually quotes customers expressing *no objection* to the use of their data for first-party marketing: “If they use the data for themselves I am fine with that.”⁵⁸

Second, the Commission itself appears to endorse this attitude, asserting that “there is a greater need to ensure express consent from an approval mechanism for third party disclosure” than for first-party marketing.⁵⁹ The proposed rules nevertheless would impose the *same* approval mechanism — opt-out for “communications-related services” and opt-in for everything else — for both uses. Nor does the Commission cite any evidence at all that customers think *broadband providers alone* should be prohibited from notifying their customers of new products, including those available from affiliates, while all others in the Internet ecosystem (and the rest of the economy) are not. This lack of evidentiary support highlights the unlawful nature of the proposed rules: there is insufficient evidence in the record to suggest that the content-based distinctions the Commission seeks to draw promote a substantial government interest,⁶⁰ and the evidence that *is* in the record shows that there is a clear mismatch between the speech restrictions and the Commission’s asserted interest.⁶¹

Third, the Commission’s proposed restriction on sharing data with affiliates makes no sense. Providers often operate under complex corporate structures that rely on affiliates to handle different but related tasks. Verizon, for example, has many separate affiliates that serve as different operating units for different parts of its business (*e.g.*, Verizon New York, Verizon

⁵⁸ *Id.*

⁵⁹ NPRM ¶ 130.

⁶⁰ *See Edenfield v. Fane*, 507 U.S. 761, 771 (1993) (invalidating speech restriction where government had “present[ed] no studies” showing that the problem the government “claim[ed] to fear” actually existed).

⁶¹ *See City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 425 (1993) (invalidating ordinance restricting commercial newsracks because “[t]he city has asserted an interest in esthetics, but respondent publishers’ newsracks are no greater an eyesore than the newsracks permitted to remain on Cincinnati’s sidewalks”).

Maryland, Cellco Partnership, AOL). One corporate affiliate may provide broadband Internet access service, but another affiliate may be responsible for billing customers or purchasing resources on behalf of another. And still another affiliate may handle marketing for all these services. Simply put, these business affiliations may serve key business and financial reporting functions that are unrelated to marketing activity and should not be disturbed. Consumers do not care about whether an affiliate or parent company handles each of these functions as long as their data is adequately protected, their choices are respected, and their services are provisioned with the quality and predictability customers expect. The broadband provider has the obligation and incentive to protect the data and to use it according to the customer's choice, and will be responsible if something happens to the data, so customers need not be concerned about where their data is held within a particular company.

Thus, as long as broadband providers (1) provide clear and transparent notices about how customer information may be used; (2) ensure that their affiliates use customer information in accordance with the choices the customer has made; (3) ensure that the affiliates secure the information appropriately; and (4) provide any required notices in the unlikely event of a breach, providers should be permitted to share their customers' information with their affiliates on an implied-consent basis. Indeed, other federal laws and regulations — including, for example, the Gramm-Leach-Bliley Act⁶² and the Fair Credit Reporting Act⁶³ — permit sharing of customer information among affiliates. Limiting the scope of implied customer consent to exclude a

⁶² See 15 U.S.C. § 6802(b)(1) (prohibiting a financial institution from disclosing “nonpublic personal information” only to a “nonaffiliated third party,” unless the consumer opts out); see also 16 C.F.R. § 313.3(m)(1) (defining “nonaffiliated third party” to mean any person except “[y]our affiliate” or “[a] person employed jointly by you and any company that is not your affiliate”).

⁶³ See 15 U.S.C. § 1681a(d)(2)(A)(ii) (excluding from the definition of “consumer report” any “communication of that information among persons related by common ownership or affiliated by corporate control”).

provider's sharing data with its affiliates will be an artificial, largely meaningless restriction with a significant compliance burden, and will serve only to increase the costs of operations for providers and the costs of services for consumers.

Finally, the Commission's proposal also improperly fails to extend certain provisions contained in the existing rules to broadband. For example, the Commission's current CPNI rules state that "[a] wireless provider may use, disclose, or permit access to CPNI derived from its provision of CMRS, without customer approval, for the provision of CPE and information service(s)."⁶⁴ There is no reason to make a distinction between wireless *voice* services and wireless *data* services, particularly where voice and data services are merging such that voice is becoming just another data application. As both Verizon and CTIA have explained in detail, the market for mobile broadband services is extremely competitive.⁶⁵ There is no reason, therefore, to distinguish between mobile broadband and mobile voice service when it comes to the using, disclosing, or permitting access to information for the purpose of marketing CPE and information services.

⁶⁴ 47 C.F.R. § 64.2005(b)(1). *See also id.* § 64.2005(c)(1), (3) (authorizing telecommunications carriers to use, disclose, and permit access to CPNI based on implied consent in its provision of inside wiring installation, maintenance, and repair services, and to market services formerly known as adjunct-to-basic services).

⁶⁵ *See, e.g.,* Comments of Verizon at 3, *Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993; Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services*, WT Docket No. 13-135 (FCC filed June 29, 2015) ("99.7 percent of the U.S. population lives in areas with mobile broadband coverage, and 93.4 percent can choose from three or more mobile broadband providers."); Comments of CTIA – The Wireless Association at 15, *Wireless Telecommunications Bureau Seeks Comment on the State of Mobile Wireless Competition*, WT Docket No. 15-125 (FCC filed June 29, 2015) ("[w]ireless mobile broadband providers are aggressively competing to offer existing and potential customers new capabilities"); *id.* at 30 ("[T]he highly competitive wireless marketplace continues to give consumers more choices for voice, data, and devices. This not only encourages wireless carriers to think of more innovative ways to promote their services, but also benefits consumers' bottom line.").

2. *The Proposed Consent Requirements for Marketing Are Unlawful*

By singling out broadband providers among similarly situated entities for special, burdensome privacy regulation, based on the mistaken view that they have unique and comprehensive access to their users' data, the Commission's proposed rules are arbitrary and capricious.⁶⁶ And, from that mistaken premise, the Commission's proposal would create an inconsistent regulatory regime that would cause consumer confusion. Further, the proposed rules directly conflict with other statutory schemes.⁶⁷ In light of the false premise behind the rules, the substantial harms to the public interest, and the lack of any identified problems with the longstanding and successful FTC privacy framework, the proposed rules are arbitrary and capricious and violate the APA.⁶⁸

More significantly, the Commission's proposal to require broadband providers to obtain opt-in consent from customers before using customer proprietary information "for any purpose" other than "marketing communications-related service[s]" violates the First Amendment.⁶⁹ The Commission's proposed rules implicate the First Amendment because they restrict "the creation

⁶⁶ See *Burlington N. & Santa Fe Ry. Co. v. Surface Transp. Bd.*, 403 F.3d 771, 777 (D.C. Cir. 2005) ("Where an agency applies different standards to similarly situated entities and fails to support this disparate treatment with a reasoned explanation and substantial evidence in the record, its action is arbitrary and capricious and cannot be upheld."); *Freeman Eng'g Assocs., Inc. v. FCC*, 103 F.3d 169, 178 (D.C. Cir. 1997) (noting that "an agency may not 'treat like cases differently'") (quoting *Airmark Corp. v. FAA*, 758 F.2d 685, 691 (D.C. Cir. 1985)); see also *Lilliputian Sys., Inc. v. Pipeline & Hazardous Materials Safety Admin.*, 741 F.3d 1309, 1313-14 (D.C. Cir. 2014) (finding agency action arbitrary and capricious where rules banned flammable gas — but not flammable gas fuel cell cartridges — from checked luggage, even though they were similar hazardous materials).

⁶⁷ The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM") requires that any sender of a commercial email provide a clear and conspicuous explanation of how the recipient can *opt out* of receiving email in the future. See 15 U.S.C. § 7704(a)(3)(A)(i).

⁶⁸ See 5 U.S.C. § 706(2)(A).

⁶⁹ NPRM ¶¶ 18, 127.

and dissemination of information,” which constitutes “speech within the meaning of the First Amendment,”⁷⁰ by prohibiting broadband providers from sending most types of marketing communications to customers without their advance, opt-in consent.⁷¹ This restriction cannot be upheld because it conflicts with controlling First Amendment standards.

The proposed rules would significantly restrict the ability of providers to use customer information in their *own* communications with their customers. The proposed rules would prohibit providers from engaging in truthful, non-misleading first-party marketing — *i.e.*, marketing conducted directly by broadband providers and their affiliates — about the vast majority of products and services, absent prior opt-in consent. And the proposed rules would also require prior opt-in consent before providers could use customer information for a wide variety of *noncommercial* purposes, such as contacting customers to make them aware of proposed legislation or regulation that could affect their interests, such as the prices of or changes to telecommunications services. These restrictions would apply even though such communications occur entirely within the provider-customer relationship, entailing *no* disclosure of customers’ information to third parties.⁷²

The proposed rules restricting first-party communications by providers with their customers violate the First Amendment because they do not advance *any* substantial or compelling government interest, much less in a narrowly tailored way.⁷³ And, because a

⁷⁰ *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011); *accord Bartnicki v. Vopper*, 532 U.S. 514, 527 (2001).

⁷¹ See NPRM ¶ 127.

⁷² *Cf. National Cable & Telecomms. Ass’n v. FCC*, 555 F.3d 996, 1002 (D.C. Cir. 2009) (“*NCTA*”) (FCC regulation “required opt-in consent only with respect to a carrier’s sharing of customer information with third-party marketers”).

⁷³ See *Sorrell*, 564 U.S. at 572; *United States v. Playboy Entm’t Group, Inc.*, 529 U.S. 803, 813 (2000).

“‘substantial number’” of the proposed rules’ “‘applications are unconstitutional,’” the restriction on providers’ use of customer information is overbroad and thus invalid in its entirety.⁷⁴

The proposed restriction on first-party marketing does not directly advance the Commission’s goals of transparency, choice, and data security.⁷⁵ It prohibits broadband providers (but not other types of commercial entities with access to the same or similar information) from *using* customer information, absent opt-in consent, to do something that businesses have done for decades: to send ads or promotions to customers for the provider’s and its affiliates’ products or services. And the proposed rules draw a distinction between first-party marketing of “communications-related services” — which requires only opt-out consent — and all other first-party marketing, which requires opt-in consent.⁷⁶

As discussed above, the Commission fails to identify any evidence supporting the content-based distinctions the proposed rules draw.⁷⁷ Moreover, customer attitudes are not a sufficient government interest to justify a flat ban on such commercial speech absent opt-in consent. The Supreme Court repeatedly has emphasized that the mere fact that certain speech may be “unwelcome” or an “annoyance” to some individuals is not an adequate constitutional ground for restricting it.⁷⁸ This is true even with respect to in-person commercial solicitation,

⁷⁴ *United States v. Stevens*, 559 U.S. 460, 473 (2010) (quoting *Washington State Grange v. Washington State Republican Party*, 552 U.S. 442, 449 n.6 (2008)).

⁷⁵ See NPRM ¶¶ 2, 5.

⁷⁶ *Id.* ¶ 127.

⁷⁷ See *supra* p. 26.

⁷⁸ *Watchtower Bible & Tract Soc’y of New York, Inc. v. Village of Stratton*, 536 U.S. 150, 168-69 (2002).

which is far more “invasive” than the type of marketing and other communications in which broadband providers and their affiliates engage.⁷⁹

The Supreme Court and other federal courts have reaffirmed advertisers’ rights to engage in marketing based on customer information in their possession. In *Shapiro v. Kentucky Bar Association*, 486 U.S. 466 (1988), the Court struck down Kentucky’s rule prohibiting attorneys from sending written advertisements to potential customers “‘precipitated by a specific event or occurrence involving or relating to the addressee . . . as distinct from the general public.’”⁸⁰ The Court rejected the argument that such a restriction was necessary to protect the public’s privacy, reasoning that “a targeted letter” does not “invade the recipient’s privacy any more than does a substantively identical letter mailed [to the public] at large.”⁸¹ “The invasion [of privacy], if any, occurs when the lawyer discovers the recipient’s legal affairs, not when he confronts the recipient with the discovery.”⁸² The same is true here: when broadband providers engage in targeted, first-party marketing efforts based on information already within their possession, customers are not adversely affected — and certainly not in such a severe way as to merit the Commission’s proposed approach of banning all such marketing absent prior opt-in consent.

Beyond the Commission’s failure to establish that its proposed rules promote a substantial government interest, the rules do not promote the asserted interest in a narrowly tailored way. The Commission does not explain why an approach similar to the FTC’s privacy

⁷⁹ See 2016 Pew Report at 6; see also *Edenfield*, 507 U.S. at 763 (invalidating ban on in-person solicitation by certified public accountants).

⁸⁰ 486 U.S. at 469-70.

⁸¹ *Id.* at 476.

⁸² *Id.*; see also *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1238-39 (10th Cir. 1999) (invalidating prior FCC rule that prohibited the use of customer information for first-party marketing); *Babkes v. Satz*, 944 F. Supp. 909, 911, 913 (S.D. Fla. 1996) (invalidating Florida statute prohibiting attorneys from sending targeted advertisements to individuals who had received traffic citations).

framework — which focuses on ensuring clear and conspicuous notice to customers and preventing misleading or deceptive practices, rather than suppressing speech — would not suffice to achieve its goals. Similarly, the Commission does not explain why the less restrictive alternative of requiring customers to opt out of receiving first-party marketing from broadband providers would not serve the Commission’s asserted interest in promoting “customers’ expectations.”⁸³ The First Amendment protects the right of commercial speakers to engage in marketing efforts *until* listeners have affirmatively chosen to opt out of receiving such communications.⁸⁴

The importance of not inhibiting any speech directed at a willing listener is substantial, because, even in the context of commercial speech, “[t]he First Amendment directs us to be especially skeptical of regulations that seek to keep people in the dark for what the government perceives to be their own good.”⁸⁵ That is especially true in the context of first-party marketing, which provides customers with truthful and accurate information about products or services in which they are likely to be interested.⁸⁶ As the Commission itself recognizes, “many consumers

⁸³ NPRM ¶ 123.

⁸⁴ *See, e.g., National Coalition of Prayer, Inc. v. Carter*, 455 F.3d 783, 789 (7th Cir. 2006) (“[T]he Supreme Court has found that statutes are not narrowly tailored when they prohibit speech to all residences where it is feasible to allow only those house-holds who do not wish to receive the speech to opt in to privacy protection.”) (citing *Playboy*, 529 U.S. at 814-15); *Mainstream Mktg. Servs., Inc. v. FTC*, 358 F.3d 1228, 1238 (10th Cir. 2004) (finding that prohibition on telemarketers calling individuals who had placed themselves on federal “Do Not Call” registry was narrowly tailored because the customer’s decision to opt in to a registry of individuals who preferred not to receive marketing communications “ensures that it does not inhibit any speech directed at . . . a willing listener”).

⁸⁵ *Sorrell*, 564 U.S. at 577 (quoting *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 503 (1996) (plurality opinion)).

⁸⁶ *See id.* at 576 (noting that marketing is often “beneficial” because consumers may “find it persuasive”); *44 Liquormart*, 517 U.S. at 503 (plurality opinion) (noting that restrictions on marketing “deprive consumers of accurate information about their chosen products”).

want targeted advertising that provides very useful information in a timely (sometimes immediate) manner.”⁸⁷

B. Restrictions on Broadband Providers’ Ability To Compete in the Digital Advertising Market Are Bad Policy, Anticompetitive, and Legally Unsupportable

1. Consumers Will Be Harmed by the Opt-In Consent Requirements for Digital Advertising

The President has “strongly encouraged” independent agencies like the Commission to “eliminate regulations that create barriers to or limit competition.”⁸⁸ But the Commission’s proposed rules would do just the opposite; as the Commission itself acknowledges, the proposed rules would create a “regulatory disparity” that will harm competition in the market for digital advertising.⁸⁹

Today’s marketplace for digital advertising is concentrated and growing more concentrated every day. Just two companies currently control almost 55% of the online advertising market and 67% of the mobile advertising market, and this share is growing with those companies controlling more than two-thirds of the growth in this market.⁹⁰ The next

⁸⁷ NPRM ¶ 12.

⁸⁸ Steps to Increase Competition and Better Inform Consumers and Workers to Support Continued Growth of the American Economy, Exec. Order No. 13,725, §§ 1, 3(b), 81 Fed. Reg. 23,417, 23,417-18 (Apr. 20, 2016).

⁸⁹ NPRM ¶ 132.

⁹⁰ See MoffettNathanson Research, *The Digital Duopoly* 1 (May 3, 2016) (“*The Digital Duopoly*”) (“After going through the report and our company/sector models, we see four key takeaways: #1: Google and Facebook drove over 2/3^{rds} of the industry’s growth in 2015 and now have almost 55% share of the digital market; #2: Mobile is now sourcing over 80% of digital’s growth; Google and Facebook also sourced 2/3rds of this market’s growth and now have 67% share of the mobile ad revenue industry; #3: Social advertising comprises over 70% of all of display’s growth . . . and Facebook has 65% share of social; #4: The shift in retailer ad spending continues to be the key driver of digital.”). See also IAB, *IAB internet advertising revenue report: 2015 full year results*, at 13 (Apr. 2016) (“IAB Advertising Report”), available at

largest player in this market holds just 4%.⁹¹ As one analyst recently noted, “[s]maller companies will continue to operate in the shadows of the industry’s two dominant players’”⁹² — which are expected to receive \$8.5 billion and \$3.8 billion, respectively, in advertising revenues this year.⁹³ And, beyond the top two digital advertisers, in 2015 the top ten Internet advertising sellers received 75% of online ad revenues (an increasing proportion over prior years).⁹⁴ None of these market leaders is a common carrier subject to the Commission’s proposed rules, as they are largely concentrated in the search engine and social media fields.

Against this backdrop, the Commission’s proposed rules would single out for heightened regulation the most likely new entrants into the digital advertising marketplace — broadband providers such as Verizon — and burden them with regulations that will not apply to the market leaders. Under the NPRM, broadband providers will face expanded opt-in requirements and a host of other regulations (such as the proposed limitations on the use of persistent identifiers and de-identified information, discussed below), while the top digital advertising sellers will remain free to access and commercialize their customers’ data without those constraints. That inconsistent approach will thwart rather than promote fair and effective competition, and will deprive customers of the benefits of a more competitive marketplace.

<http://www.iab.com/wp-content/uploads/2016/04/IAB-Internet-Advertising-Revenue-Report-FY-2015.pdf>.

⁹¹ See *The Digital Duopoly* at 2.

⁹² Aleksandra Gjorgievska, *Google and Facebook Lead Digital Ad Industry to Revenue Record*, Bloomberg (Apr. 21, 2016), <http://www.bloomberg.com/news/articles/2016-04-22/google-and-facebook-lead-digital-ad-industry-to-revenue-record>.

⁹³ See eMarketer Inc., *Facebook and Twitter Will Take 33% Share of US Digital Display Market by 2017* (Mar. 26, 2015), <http://www.emarketer.com/Article/Facebook-Twitter-Will-Take-33-Share-of-US-Digital-Display-Market-by-2017/1012274>.

⁹⁴ See IAB Advertising Report at 11.

2. *The Opt-In Consent Requirements for Digital Advertising Are Unlawful*

The Commission’s proposed rules violate the First Amendment because they would require opt-in consent for *any* disclosure of *any* customer proprietary information by a broadband provider to *any* third party.⁹⁵ As the *Sorrell* Court recognized, the “dissemination of information” to third parties is protected by the First Amendment.⁹⁶ The Commission cannot carry its burden of demonstrating that this broad type of opt-in regime, rather than some form of opt-out regime, is necessary to achieve its goals of privacy, choice, transparency, and security.⁹⁷

As an initial matter, the proposal to require opt-in consent for disclosure of all customer proprietary information to third parties is subject to strict scrutiny, because the Supreme Court’s “precedents define commercial speech as ‘speech that does no more than propose a commercial transaction.’”⁹⁸ Unlike marketing, the sharing or disclosing of customer proprietary information to third parties does not propose any commercial transaction. Thus, in *Sorrell*, the Supreme Court noted that it was unclear whether the “speech hampered by” Vermont’s law prohibiting the disclosure of prescription information to pharmaceutical marketers “is commercial, as our cases have used that term.”⁹⁹ Here, the Commission’s proposed rules go even further than the Vermont law at issue in *Sorrell*: they prohibit disclosure or sharing of customer proprietary information with *all* third parties, including those who have no commercial purpose at all, such

⁹⁵ See NPRM ¶ 127.

⁹⁶ 564 U.S. at 570.

⁹⁷ See NPRM ¶¶ 2, 5.

⁹⁸ *Harris v. Quinn*, 134 S. Ct. 2618, 2639 (2014) (quoting *United States v. United Foods, Inc.*, 533 U.S. 405, 409 (2001)).

⁹⁹ 564 U.S. at 571.

as academic researchers.¹⁰⁰ Strict scrutiny, rather than a commercial speech inquiry, is thus required. Yet, as in *Sorrell*, “the outcome is the same whether a special commercial speech inquiry or a stricter form of judicial scrutiny is applied.”¹⁰¹

The Commission’s proposed rules fail to satisfy the *Sorrell/Central Hudson*¹⁰² test: they do not “directly advance[] a substantial governmental interest” and are not narrowly “drawn to achieve that interest.”¹⁰³ That is because the Commission’s choice of an opt-in regime does not promote the Commission’s “core” privacy principles of choice and transparency.¹⁰⁴ An opt-in regime does not advance these interests any more than a well-designed opt-out regime would.

Multiple courts have recognized that an agency’s choice of an opt-in regime rather than an opt-out regime presents First Amendment concerns in the context of restrictions on telecommunications carriers’ use or disclosure of customer data. In *U.S. West*, the Tenth Circuit invalidated a Commission regulation requiring carriers to obtain opt-in consent prior to using or sharing customer data.¹⁰⁵ The court reasoned that the Commission had “fail[ed] to adequately consider an obvious and substantially less restrictive alternative, an opt-out strategy.”¹⁰⁶ The court rejected the Commission’s “speculat[ion] that there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the

¹⁰⁰ *Cf. id.* at 563 (Vermont law contained exception permitting disclosure to academic researchers).

¹⁰¹ *Id.* at 571.

¹⁰² *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm’n of New York*, 447 U.S. 557 (1980).

¹⁰³ *Sorrell*, 564 U.S. at 572; accord *Greater New Orleans Broad. Ass’n, Inc. v. United States*, 527 U.S. 173, 188 (1999).

¹⁰⁴ NPRM ¶ 5.

¹⁰⁵ See 182 F.3d at 1229.

¹⁰⁶ *Id.* at 1238.

opportunity to do so.”¹⁰⁷ “Such speculation,” the court concluded, “hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires.”¹⁰⁸

Here, the Commission has not offered an adequate explanation of why an opt-out regime — which all of the cases above deemed essential from a First Amendment standpoint — would not suffice to achieve its aims. To justify its choice of an opt-in regime, the Commission relies primarily on the aforementioned 2016 Pew Report.¹⁰⁹ Nothing in the report, however, suggests that customers view an opt-out regime as insufficient to protect their information; just the opposite.¹¹⁰ Beyond the unsupportive Pew Report, the Commission “provides no additional evidence” to justify its choice.¹¹¹

The Commission fails to explain why even a well-crafted, clear, and conspicuous opt-out notice would not give customers “*the opportunity* to affirmatively choose how their information

¹⁰⁷ *Id.* at 1239.

¹⁰⁸ *Id.* See also *Verizon Northwest, Inc. v. Showalter*, 282 F. Supp. 2d 1187, 1194 (W.D. Wash. 2003) (rejecting the agency’s preference for an op-in regime, reasoning that “it is evident that the *presentation* and *form* of opt-out notices is what determines whether an opt-out campaign enables consumers to express their privacy preferences,” as reflected in the Commission’s own extensive requirements relating to the “the form, content, and frequency of opt-out notices”); *id.* at 1194-95 (“properly controlled opt-out campaigns can protect consumers . . . without impacting speech to the extent” that an opt-in regime does); *Mainstream Mktg.*, 358 F.3d at 1242-43 (Tenth Circuit upholding Do Not Call registry because the opt-out nature of the restriction on telemarketers contacting individuals “render[ed] it a narrowly tailored commercial speech regulation,” because “the Supreme Court has often reasoned” that a regulation allowing individuals to opt out of receiving communications “would have been a less restrictive alternative” than regimes requiring prior opt-in consent). The Seventh Circuit adopted similar reasoning in upholding as narrowly tailored an Indiana law prohibiting charities from using telemarketers to call residents who had placed themselves on the State’s do-not-call list. See *National Coalition of Prayer*, 455 F.3d at 784, 792.

¹⁰⁹ See NPRM ¶ 129 n.226.

¹¹⁰ See 2016 Pew Report at 24 (customer expressing desire for ability to “*opt out* on sharing with third parties”) (emphasis added); *id.* at 33 (customer stating that “[i]f I *have the option* to suppress my email address and turn off advertisements, then I would join the site”) (emphasis added).

¹¹¹ *U.S. West*, 182 F.3d at 1239.

is used.”¹¹² Indeed, the Commission expressly recognizes the possibility of designing “a standardized template for privacy notices” that would be easily read and understood by customers,¹¹³ but fails to explain why a template of this sort under an opt-out regime would be inadequate.¹¹⁴ The Commission’s failure to explain why a clear and conspicuous opportunity to opt out would be inadequate is particularly telling in light of the fact that multiple other federal statutes and regulations rely on just such a regime.¹¹⁵ And the Commission’s failure adequately to justify its choice of an opt-in regime is especially problematic given the extremely broad reach of the proposed rules: they would prohibit a broadband provider even from sharing a customer’s information with affiliates and contractors under contractual agreements with the provider for work associated with keeping customer data private and secure. Indeed, the proposed rules would even restrict broadband providers from sharing such information for purposes of data analysis in anticipation and support of the providers’ *own* marketing efforts, a widespread and routine industry practice that is entitled to First Amendment protection under *Sorrell*.¹¹⁶

¹¹² NPRM ¶ 127 (emphasis added).

¹¹³ *Id.* ¶ 91.

¹¹⁴ *Cf. Verizon Northwest*, 282 F. Supp. 2d at 1194 (rejecting argument that no conceivable opt-out notice could be designed such that customers would “see,” “read,” and “understand” it); *Playboy*, 529 U.S. at 824 (concluding that the government had failed to show that an “adequately advertised” opt-out mechanism for sexually explicit television channels “would not be effective” in allowing parents to prevent their children from viewing such channels).

¹¹⁵ *See, e.g.*, 15 U.S.C. § 6802(b)(1)(A) (Gramm-Leach-Bliley Act requires financial institutions to give customers “clear[] and conspicuous[]” notice and opportunity to opt out before nonpublic personal information is shared with third parties); 47 C.F.R. § 64.1200(a)(4) (FCC regulation implementing Telephone Consumer Protection Act of 1991 requires fax advertisements to include notice and opportunity to opt out).

¹¹⁶ *See* 564 U.S. at 564 (noting that a law that “bars any disclosure” of information where that information will ultimately be “use[d] . . . for marketing . . . disfavors marketing” and thus constitutes a content-based speech restriction).

The Commission’s proposed rules would prohibit broadband providers not just from obtaining customers’ consent through unfair or deceptive means; it would prohibit them from using even *clear, conspicuous, and fair* opt-out notices to obtain customer consent. This plainly violates the First Amendment. The FTC enforces no comparable restriction on edge providers or mobile operating system providers (nor did it ever do so on broadband providers). While it may be true that “large edge providers are increasingly adopting opt-in regimes for sharing of some types of sensitive information,”¹¹⁷ so, too, have broadband providers adopted opt-in regimes for sensitive data.¹¹⁸ This fact further underscores how the Commission’s broader approach restricts more speech than necessary to accomplish its goals.

3. *Prohibitions on “Persistent Identifiers” and “Deep-Packet Inspection” Would Harm Competition*

The Commission should not prohibit the use of two specific technologies — unique advertising identifiers and deep-packet inspection. As with determining what notice-and-choice requirements should apply to broadband providers, the touchstone of the Commission’s analysis with respect to what technologies should be allowed should be to ensure that consumers’ privacy is protected by a consistent regime that applies equally to all players in the ecosystem.

While the Commission calls them “persistent tracking technologies,”¹¹⁹ these technologies are actually just anonymous identifiers that are used to support mobile online

¹¹⁷ NPRM ¶ 132.

¹¹⁸ *See, e.g.*, Advertising Appendix at 6 (“Because this program uses more sensitive customer data, customers are enrolled in Verizon Selects only if they affirmatively opt in to the program.”).

¹¹⁹ NPRM ¶ 268.

advertising. Depending on how the identifier is set up, they may – or may not – be “persistent.”¹²⁰

Advertising identifiers are common tools in digital advertising as they help ensure customers receive advertisements that are more appealing to them. Other companies that will not be subject to the rules proposed in the NPRM, including edge providers and mobile operating system providers, also use advertising identifiers in their targeted advertising programs.¹²¹ Prohibiting broadband providers from also doing so, without articulating a reason why this distinction is necessary, will be competitively harmful and discriminatory to these companies. And, in any event, consumers *benefit* from the use of these identifiers both through any inducements that may be offered for their use and because the advertising identifiers make it more likely that a consumer will receive advertisements that are actually of interest to the consumer.

Advertising identifiers permit marketers to provide useful information to an anonymous customer in a way that protects the privacy of individuals. If customers are going to receive advertisements while using the Internet — and they certainly are, given the wide range of Internet services that operate on an advertising model — advertising identifiers help ensure advertisers can provide more relevant advertising to Internet users while the advertiser never receives or learns the actual identities of those users.

¹²⁰ Although the Commission describes Verizon’s UIDH as a persistent identifier, *see* NPRM ¶ 268, Verizon disagrees — the UIDH changes regularly, without customer intervention. Ultimately, the nomenclature is irrelevant, and advertising identifiers like the UIDH should be permitted for the reasons described above.

¹²¹ Both Apple and Google use advertising identifiers to serve advertisements to users on mobile devices, but, unlike Verizon, they do not proactively change the identifier regularly; instead, if a customer wants to change her identifier, she must reset it manually. Verizon also offers the ability to block transmission of its identifier entirely, which is not a choice made available for these other advertising identifiers.

Verizon’s own advertising programs use an anonymous identifier, known as the UIDH, as well as other online and device identifiers.¹²² Verizon designed the UIDH to be more protective of consumer privacy interests than many of these other advertising identifiers. Each UIDH is a unique character string, indistinguishable from a random string of data, that changes automatically, without intervention from the customer. The UIDH does not reveal any personally identifiable information (“PII”). Verizon limits the sharing of such identifiers to its own affiliates, so they are not shared with third parties without the customer’s opt-in consent.¹²³ In addition, Verizon recognizes that some customers might prefer not to participate in such programs, and provides a means for those consumers to opt out of those programs. Unlike other advertising identifiers, Verizon’s UIDH is not transmitted for consumers who opt out of Verizon’s advertising programs.¹²⁴ Thus, advertising identifiers can be — and often are — used in a way that protects and promotes consumer privacy, and there is no reason to ban their use by broadband providers.

The Commission similarly should not prohibit the use of so-called “deep-packet inspection” by ISPs.¹²⁵ As the Commission describes it, deep-packet inspection refers to any technology that provides the ability to look into the packet past the basic header information and includes any inspection of packets beyond looking at the top-level domain name, even if the substantive contents of the packets are not reviewed. Other providers in the Internet ecosystem, which are subject to the FTC’s regime, actually review the contents of the packets and information they receive. For example, some providers review emails or social media posts to

¹²² See Advertising Appendix at 3-4.

¹²³ *Id.* at 6-7.

¹²⁴ *Id.*

¹²⁵ See NPRM ¶ 264.

provide advertising alongside a user's inbox or news feed, or track which stories users are reading. Yet a prohibition on "deep-packet inspection," in the broad way the Commission defines it, would reach much less invasive practices.

With respect to packet header information, the collection and use of that data should be subject to general rules already discussed. For example, if that information is used in aggregate and de-identified form, ISPs should face no limitations on the use of technologies that facilitate the collection of the information. If, on the other hand, that information is used to target ads to specific individuals, the sensitivity of that information supports a requirement to secure a customer's opt-in consent for that use.

There is no reason why ISPs should be subject to a unique prohibition on the use of a technology for any purpose. So long as customers are given notice about a broadband provider's practices and a fair opportunity to consent to the practice, there is no reason for this rigid, categorical ban. For example, Verizon commits in its privacy policy to obtain opt-in consent before it will "use information . . . gathered in the course of providing broadband Internet access services about [a customer's] visits over time to different non-Verizon websites to customize ads."¹²⁶ And Verizon only uses information about a customer's browsing to deliver targeted advertising where customers have opted in.¹²⁷

Finally, a prohibition on deep-packet inspection risks cutting off future innovations and the development of potentially valuable products for consumers. There is no way for the Commission to know whether deep-packet inspection could form a foundation for a new set of services ISPs could offer to their customers. For example, parents could place great value on a

¹²⁶ Verizon, "Full Privacy Policy," <http://www.verizon.com/about/privacy/full-privacy-policy>.

¹²⁷ See Advertising Appendix at 6-7.

service that lets them know if the content of a child’s communications has strayed into a set of worrisome topics. Such services should be subject to appropriate privacy rules, but a flat technological prohibition applied only to a small set of participants in the market is not good policy.

4. *Appropriate Use of De-Identified Customer Information Should Not Be Restricted*

Broadband providers should be permitted to use and, in appropriate circumstances, share de-identified customer information. So long as certain guidelines are followed, de-identified data does not pose the same risks as identified data. Indeed, if data cannot be reasonably re-identified, either because the data is not linkable to an individual or because the provider and its contractors have committed not to re-identify the data, there is no privacy risk to consumers as they cannot be associated with that data. Thus, the permission to use and disclose de-identified data should not depend on whether the data is in the aggregate or in an individual de-identified form.

Instead, providers should be allowed to use and disclose individual de-identified data as long as the provider — and anyone it shares the data with — honors a consumer’s choices prior to using that data in a way that would target the customer. For example, providers should contractually prohibit any entity with which it shares individual de-identified data from using that data for their own purposes and from attempting to associate that data with particular consumers. Providers also should exercise reasonable monitoring to ensure these contracts are not violated. In addition, providers should not be allowed to re-identify consumer data and then use that re-identified data to target customers that have otherwise opted out or not opted in to particular uses of their individualized data. In other words, providers should not be allowed to use de-identification and re-identification to circumvent consumers’ privacy choices. However,

to the extent a customer has consented to the use of his or her underlying individualized data, the provider should not lose the ability to use that data just because it de-identifies the data for added protection in some contexts. What matters is that the provider’s use of consumer data remains consistent with the customer’s choices.¹²⁸

C. Prohibiting Financial Inducements Would Be Both Unwise and Unlawful

The Commission’s criticism of “financial inducements”¹²⁹ ignores how the Internet economy works. Companies give away email, search functionality, mapping, and much else in exchange for information used to serve ads. Social networks do the same. Content publishers make news, videos, and entertainment available in return for obtaining consumer information and serving ads. This is widely beneficial for consumers and businesses alike. The notion that ISPs should be uniquely prohibited from participating in this kind of value exchange is terrible policy.

Prohibiting ISPs from offering similar consumer benefits would disadvantage consumers who would like to make an informed choice whether to allow a reasonable level of third-party access and use of their information in exchange for financial or other benefits. The evidence suggests that a substantial number of customers — likely a majority — would fall into this category and would benefit from having this choice regarding the use of their data.¹³⁰ Survey and market-research data indicate that consumers are willing to make a reasoned decision to

¹²⁸ For example, if the carrier de-identifies data to add protection in some contexts — such as where a third party is doing list matching based on an email address — that should not preclude the carrier from using the underlying data in a way that is consistent with the consumers’ expressed preferences, *e.g.*, re-identifying the data to serve more effective and relevant advertisements.

¹²⁹ *See* NPRM ¶¶ 259-263.

¹³⁰ *See id.* ¶ 259 (recognizing that a “substantial majority” of eligible customers have elected to participate in AT&T’s program offering discounts in exchange for permission to use web-browsing information).

share certain types of information with advertisers in exchange for discounts and other financial benefits.¹³¹ Indeed, they do this every day, as they participate in discount and loyalty programs in their neighborhood grocery stores and pharmacies. In addition to the financial benefit of lower-priced services, these consumers clearly prefer to receive targeted advertisements for products or services that are more likely to interest them.¹³² The Commission should not prohibit or regulate such offerings, which give consumers the benefit of valuable free or discounted services based on an informed choice on how they may benefit from the use of their data. Prohibiting such programs contradicts not only the principle of choice enshrined in Section 222, but common sense as well.¹³³

In any event, the Commission lacks the power to restrict or ban broadband providers from offering customers financial inducements or other things of value, such as loyalty program benefits, for permission to use or share customer proprietary information. The NPRM fails to explain what source of statutory authority the Commission believes supports the proposed financial-inducement ban. The Commission relies on Section 222 as the primary source of legal

¹³¹ See, e.g., PwC, *The Speed of Life: Consumer Intelligence Series 2-3* (2012) (finding that 73% of survey respondents were willing to share personal information in exchange for financial benefits, with consumers expressing greater willingness to share information in exchange for large benefits like “[a] free timeshare” than for smaller benefits like “a free candy bar”), <http://www.pwc.com/us/en/industry/entertainment-media/assets/pwc-consumer-privacy-and-information-sharing.pdf>; McCann Worldgroup, *The Truth About Privacy* 11 (2011) (finding that 65% of consumers view discounts as a major “benefit[.]” of sharing information and that customers are more willing to share less-sensitive information like shopping history and location data than more-sensitive information like medical or financial data), http://mccann.com/wp-content/uploads/2012/06/McCann_Truth_about_Privacy.pdf.

¹³² See NPRM ¶ 12 (noting that “many consumers want targeted advertising that provides very useful information”); cf. *Sorrell*, 564 U.S. at 576 (noting that customers often find advertising “persuasive”).

¹³³ For these same reasons, the Commission’s prohibition on financial inducements is arbitrary and capricious, for the rules “have no connection to the goals” of promoting consumer choice that underlie the regulation. See *Judulang v. Holder*, 132 S. Ct. 476, 487 (2011).

authority underlying the NPRM,¹³⁴ but also cites its general authority to “‘prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of’” the Communications Act.¹³⁵ But neither Section 222 nor the Commission’s general regulatory power provides a basis for the financial-inducement ban. Prohibiting financial inducements also would violate the First Amendment.

1. Section 222 Does Not Authorize the Commission To Prohibit Consumers from Receiving Benefits in Exchange for Allowing Use of Their Information

Nothing in Section 222 says anything about financial inducements, discounts, or pricing, and the Commission does not argue otherwise. In fact, the proposed financial-inducement ban would *restrict* consumer choice, contrary to the fundamental premise of Section 222. Indeed, the Commission recognizes that “[c]ustomer approval is a key component of the privacy framework of Section 222.”¹³⁶ Section 222’s provisions relating to the confidentiality of CPNI contain an express exception allowing CPNI to be used and disclosed “with the approval of the customer.”¹³⁷ Multiple other provisions of the section also emphasize consumer choice and approval.¹³⁸ These provisions make clear that Congress envisioned a regime in which customers would have the option to consent to the use or disclosure of their personal information. The

¹³⁴ See NPRM ¶ 294.

¹³⁵ *Id.* ¶¶ 295 n.457, 305-306 (quoting 47 U.S.C. § 201(b)); see also 47 U.S.C. §§ 154(i), 303(r) (providing similar authority).

¹³⁶ NPRM ¶ 302.

¹³⁷ 47 U.S.C. § 222(c)(1).

¹³⁸ See *id.* § 222(c)(2) (“A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.”); *id.* § 222(d)(3) (discussing customer approval in context of “inbound telemarketing, referral, or administrative services”); *id.* § 222(f)(1) (discussing customer approval to use location information).

proposed financial-inducement ban would be an obstacle to that goal, not an aid to it, and would violate the plain language of Section 222.

2. *Section 201(b) Does Not Authorize the Commission To Prohibit Consumers from Receiving Benefits in Exchange for Allowing Use of Their Information*

The Commission cannot fall back upon its general regulatory authority under Section 201(b) or similar provisions of the Communications Act. Section 201(b) allows the Commission to regulate where “necessary . . . to carry out the provisions of [the Act].”¹³⁹ But, as discussed above, the financial-inducement ban cannot be said to carry out Section 222, because it *contradicts* Section 222’s emphasis on customer choice and consent. Courts have recognized that the Commission cannot use its general regulatory authority under the Communications Act to enact regulations that conflict with congressional intent reflected in other provisions of the Act.¹⁴⁰ The Commission cannot use its authority under Section 201(b) to circumvent Congress’s desire to empower customers and promote choice.

The Commission also suggests that the rules proposed in the NPRM generally may be justified under Section 201(b)’s separate prohibition on “practices . . . in connection with [a] communication service” that are “unjust or unreasonable.”¹⁴¹ But the Commission cannot deem

¹³⁹ *Id.* § 201(b).

¹⁴⁰ *See FCC v. Midwest Video Corp.*, 440 U.S. 689, 691, 706-07 (1979) (notwithstanding fact that the statutory provision at issue did not “explicitly limit the regulation of cable systems,” the Commission “was not delegated unrestrained authority” and was not free to disregard other provisions of the Act evincing Congress’s desire to preclude the Commission from imposing common-carrier-type regulations on cable companies); *see also, e.g., Texas Office of Pub. Util. Counsel v. FCC*, 183 F.3d 393, 423 (5th Cir. 1999) (holding that Commission “cannot use its normally broad regulatory authority” under Section 201(b) to “override” statutory provision restricting the Commission’s jurisdiction over intrastate activities).

¹⁴¹ 47 U.S.C. § 201(b). The NPRM does not expressly contend that the proposed financial-inducement ban can be justified under this provision, *see* NPRM ¶ 306 (arguing only that “Section 201 of the Communications Act and Section 5 of the FTC Act can be read as

the practice of offering financial inducements unjust or unreasonable where the practice is *consistent* with the principle of choice enshrined in Section 222.¹⁴² The serious First Amendment concerns raised by the proposal, *see infra* pp. 50-53, also highlight its unlawful nature. While the Commission’s determination of what practices are “unjust” or “unreasonable” ordinarily receives *Chevron* deference,¹⁴³ such deference is inappropriate where, as here, the Commission’s interpretation raises “constitutional questions” (in this case, under the First Amendment).¹⁴⁴

The Commission’s proposal also finds no support in precedent. The offering of benefits to customers, including “financial inducements,” loyalty rewards, or other things of value, to customers in exchange for permission to use or disclose customer proprietary information is not on its face an unjust or unreasonable practice, and it is not comparable to the types of practices the Commission has determined to be “unjust or unreasonable” in the past. For instance, in the FCC/FTC Joint Policy Statement cited by the Commission,¹⁴⁵ the agencies targeted vendors of long-distance calling services who had engaged in “misleading” and “deceptive” marketing practices.¹⁴⁶ The NPRM does not suggest that broadband providers have engaged, or would

prohibiting the same types of acts or practices” — those that are “unfair or deceptive” and “unjust, unreasonable, or unreasonably discriminatory”).

¹⁴² *See Metrophones Telecomms., Inc. v. Global Crossing Telecom., Inc.*, 423 F.3d 1056, 1068 (9th Cir. 2005) (noting that “there are statutory constraints on the Commission’s power to deem a practice ‘unjust’ and ‘unreasonable’”), *aff’d*, 550 U.S. 45 (2007).

¹⁴³ *See Capital Network Sys., Inc. v. FCC*, 28 F.3d 201, 204 (D.C. Cir. 1994).

¹⁴⁴ *Bell Atl. Tel. Cos. v. FCC*, 24 F.3d 1441, 1443, 1446-47 (D.C. Cir. 1994) (finding lack of statutory authority to issue regulation in light of the “constitutional implications of the Commission’s action”).

¹⁴⁵ *See NPRM* ¶ 306 n.474.

¹⁴⁶ Joint FCC/FTC Policy Statement for the Advertising of Dial-Around and Other Long-Distance Services to Consumers, 65 Fed. Reg. 44,053, 44,054 (July 17, 2000); *see also, e.g.*,

engage, in misleading or deceptive advertising of financial-inducement offers, nor does the NPRM explain why any hypothetical customer confusion¹⁴⁷ could not be addressed through clear and conspicuous disclosure of the terms of financial-inducement offers.

3. *Prohibiting Financial Inducements Violates the First Amendment*

In addition to exceeding the Commission's power under the Communications Act, the proposed ban on financial inducements also would violate the First Amendment. The proposal implicates the First Amendment because, as multiple courts have recognized, the offering of discounts or promotions to customers is communicative in nature: it is a critical tool for conveying information about prices and to draw customers' attention to particular products or services in which they may be interested. Here, the Commission proposes to restrict discounting out of a fear that the communication will prove *too persuasive* and will convince many customers to agree to share their data. The *Sorrell/Central Hudson* test thus applies, and the Commission's proposal fails to satisfy that test because it does not advance the government's asserted interests in customer choice and transparency. On the contrary, the proposal actually *harms* those interests: by prohibiting customers from obtaining any financial benefit from allowing their information to be used or disclosed, the proposal aims to keep customers in the dark about the economic value of their data and to burden their ability to agree to share it.

In recent years, multiple federal courts have been confronted with First Amendment challenges to laws restricting both the offering and the advertising of price discounts.¹⁴⁸ The

FTC v. Verity Int'l, Ltd., 443 F.3d 48, 54-55 (2d Cir. 2006) (enforcement action against company engaged in deceptive billing practices for dial-up internet service).

¹⁴⁷ See NPRM ¶ 260.

¹⁴⁸ Compare, e.g., *Discount Tobacco City & Lottery, Inc. v. United States*, 674 F.3d 509, 543-44 (6th Cir. 2012) (invalidating ban on tobacco loyalty discounts), and *Dana's R.R. Supply v. Attorney General of Florida*, 807 F.3d 1235, 1251 (11th Cir. 2015) (invalidating Florida law that banned "surcharges" for credit-card users but allowed merchants to offer "discounts" to

outcomes in these cases have turned primarily on whether, in the court’s view, the law at issue sought to regulate the “‘communicative impact’” of the pricing discount¹⁴⁹ or whether the law instead amounted to a purely economic regulation akin to “price-control laws,” which generally do not implicate the First Amendment.¹⁵⁰ These cases rely on the Supreme Court’s oft-repeated rule that, where a government regulation seeks to restrict *conduct* that also expresses communicative content, “[i]t may not . . . proscribe particular conduct *because* it has expressive elements.”¹⁵¹

In this case, the Commission’s proposal implicates the First Amendment because it would regulate the financial-inducement practices of broadband providers (and only broadband providers) because of their communicative content — namely, their power to persuade customers to agree to share their information. The Commission contends that, “[n]otwithstanding the prevalence of such practices in other contexts,” it is “not clear that consumers generally understand that they are exchanging their information as part of those bargains.”¹⁵² In other words, the Commission contemplates banning the offering of discounts not for any reason related to the economic impacts of those discounts, but to prevent broadband providers from persuading customers to agree to share their information.

customers paying with cash), *with National Ass’n of Tobacco Outlets, Inc. v. City of Providence*, 731 F.3d 71, 78 (1st Cir. 2013) (upholding ban on tobacco price discounts), *and Rowell v. Pettijohn*, 816 F.3d 73, 78, 83 (5th Cir. 2016) (describing “circuit split” on the issue and upholding Texas law banning price surcharges for credit-card customers).

¹⁴⁹ *Discount Tobacco*, 674 F.3d at 539 (quoting *Lorillard Tobacco Co. Reilly*, 533 U.S. 525, 567 (2001)).

¹⁵⁰ *Rowell*, 816 F.3d at 82 (citing *Nebbia v. New York*, 291 U.S. 502, 537 (1934)).

¹⁵¹ *Texas v. Johnson*, 491 U.S. 397, 406 (1989); *see also, e.g., Lorillard*, 533 U.S. at 567 (government interest underlying regulation of expressive conduct must be “unrelated to expression”).

¹⁵² NPRM ¶¶ 260-261.

The Commission’s proposal implicates important First Amendment interests for a separate but related reason: just as it would restrict the ability of broadband providers to engage in expression, so too would it burden *customers’* decisions to agree to the use and disclosure of their information to third parties. The Supreme Court has repeatedly held that laws prohibiting individuals from receiving compensation for engaging in speech implicate the First Amendment.¹⁵³

For all these reasons, the proposed financial-inducement restriction requires First Amendment scrutiny and must (at least) survive the *Sorrell/Central Hudson* test. The proposal fails that test because it does not advance any substantial government interest and is not narrowly tailored. Not only does the proposal not promote the values of “choice” and “transparency” the Commission has identified,¹⁵⁴ it inhibits those interests. The proposal would prohibit customers — even fully informed, knowledgeable customers — from choosing to allow broadband providers to use or disclose their information in exchange for a discount. The NPRM fails to explain how a restriction that would thwart the will of a majority of customers can be said to promote customer choice.¹⁵⁵ The Commission’s proposal also hinders its own stated goal of

¹⁵³ See *United States v. National Treasury Emps. Union*, 513 U.S. 454, 457 (1995) (invalidating on First Amendment grounds a law prohibiting federal employees “from accepting any compensation for making speeches or writing articles”); *id.* at 468 (a “prohibition on compensation” for individuals who choose to speak “unquestionably impose[d] a significant burden” on free speech, requiring First Amendment scrutiny); *id.* at 469 (because “compensation provides a significant incentive toward more expression, ... [b]y denying [the employees] that incentive, the honoraria ban induces them to curtail their expression,” burdening their free speech).

¹⁵⁴ NPRM ¶¶ 2, 5.

¹⁵⁵ The available evidence suggests that most customers would choose to accept a discount in exchange for the use of their data, if it were offered. See NPRM ¶ 259 (noting that a “substantial majority” of AT&T customers elected to participate in its discount program).

transparency, by preventing broadband providers from sending accurate price signals to customers about the value that providers and other third parties place on access to their data.¹⁵⁶

Finally, if the Commission’s concern is that some customers do not “understand” the nature of the discounts, or that they are not “fully informed about the privacy rights they [may be] exchanging for a discounted broadband price,”¹⁵⁷ the appropriate solution to that hypothetical problem would be clear and conspicuous disclosure or a public-information campaign, not a ban on the underlying transaction.¹⁵⁸ The Commission may disagree with the choices some individuals would make to allow sharing of their data, but the “fear that people would make bad decisions if given truthful information” is not an adequate ground for restricting speech.¹⁵⁹

D. The Statute Provides the Commission with Authority over CPNI, Not All Consumer Data

1. Section 222(a) Only Applies to CPNI

The Commission has long understood Section 222, as it applies to retail customers’ information, to be limited to CPNI.¹⁶⁰ The Commission’s novel conclusion that Section 222(a) reaches beyond CPNI and allows the Commission to impose similar obligations on carriers with respect to a wide range of additional information that is not CPNI cannot be squared with that history, with the text or structure of the statute, or with Congress’s repeated decision to use the

¹⁵⁶ See *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 765 (1976) (“free flow” of price information is “indispensable” to proper functioning of our “predominantly free enterprise economy”).

¹⁵⁷ NPRM ¶¶ 260, 263.

¹⁵⁸ See, e.g., *Sorrell*, 564 U.S. at 578 (discussing “prescription drug educational program”); *Playboy*, 529 U.S. at 824 (discussing “adequately advertised” opt-out option as a more narrowly tailored alternative).

¹⁵⁹ *Thompson v. Western States Med. Ctr.*, 535 U.S. 357, 374 (2002).

¹⁶⁰ Of course, the Commission can only apply the provisions of Section 222 that apply to common carriers if it is found properly to have re-classified both fixed and mobile broadband Internet access service as a common-carrier service in the *Open Internet Order*.

phrase “personally identifiable information” when it intended to protect such information, including elsewhere in the Communications Act. Nor does any other provision of the Communications Act give the Commission authority to extend the requirements of Section 222 to reach retail customer information that is not CPNI.

Section 222 is the sole provision of the Communications Act that regulates customer information, and it is limited to CPNI. The background and enactment of Section 222 confirms this. Before the Telecommunications Act of 1996 (“1996 Act”), the Commission “established requirements applicable to the use of CPNI for the marketing of enhanced services and [customer premises equipment] by AT&T, the [Bell Operating Companies (‘BOCs’)], and GTE”¹⁶¹ in the *Computer II*¹⁶² and *Computer III*¹⁶³ proceedings. In the 1996 Act, Congress extended that regime and “established requirements for maintaining the confidentiality of CPNI . . . for all telecommunications carriers.”¹⁶⁴ Thus, rather than broadly authorizing the Commission to adopt regulations governing private customer information, Congress simply expanded the existing CPNI protections to all telecommunications carriers, including the new entrants the 1996 Act envisioned.

¹⁶¹ See Notice of Proposed Rulemaking, *Implementation of the Telecommunications Act of 1996*, 11 FCC Rcd 12513, ¶ 4 (1996) (“1996 CPNI NPRM”).

¹⁶² See, e.g., Final Decision, *Amendment of Section 64.702 of the Commission’s Rules and Regulations (Second Computer Inquiry)*, 77 F.C.C.2d 384, ¶ 249 (1980) (“[I]nformation which finds a principal use in marketing, such as customer proprietary information, must be disclosed to other competitive vendors at the same time the subsidiary receives the information and under the same terms and conditions if it is shared with the subsidiary.”).

¹⁶³ See, e.g., Report and Order, *Amendment of Section 64.702 of the Commission’s Rules and Regulations (Third Computer Inquiry)*, 104 F.C.C.2d 958, ¶ 224 (1986) (“[W]ith respect to CPNI, we require AT&T to make such information available to any enhanced services vendor at the customer’s request and to provide confidential treatment for CPNI at the customer[’]s request.”).

¹⁶⁴ 1996 CPNI NPRM ¶ 8 (emphasis added).

Furthermore, in defining the scope of the CPNI that Section 222 would protect, Congress at first considered a broad approach. The House’s original bill defined CPNI to include “such other information concerning the customer as is available to the local exchange carrier” and permitted the Commission to define the term further according to the public interest.¹⁶⁵ Similarly, the Senate’s version stated that Section 222 applied broadly to “customer-specific proprietary information.”¹⁶⁶ Congress ultimately rejected both approaches, instead choosing to define the scope of Section 222 narrowly in Section 222(h)(1), which specifically defines CPNI as information, other than subscriber list information (itself a defined term), that:

relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; [or is] contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.¹⁶⁷

Notably absent from the definition of CPNI are any open-ended terms for the Commission to define through regulation to expand the scope of protected information beyond the specifically included items.

For 18 years, the Commission recognized that Section 222, as it applies to retail customers, is limited to CPNI.¹⁶⁸ In 1998, shortly after Section 222 was enacted, the Commission explained that the section “sets forth three categories of customer information to which different privacy protections and carrier obligations apply — individually identifiable

¹⁶⁵ H.R. Rep. No. 104-204, pt. 1, at 23 (1995).

¹⁶⁶ S. Rep. No. 104-23, at 24 (1995).

¹⁶⁷ 47 U.S.C. § 222(h)(1).

¹⁶⁸ *See 1996 CPNI NPRM* ¶ 2 (“Section 222 [of] the Communications Act . . . sets forth, among other things, restrictions on the use of CPNI”).

CPNI, aggregate customer information, and subscriber list information.”¹⁶⁹ In 1999, the Commission denied a “request that the Commission hold that section 222 controls all issues involving customer information, rather than issues pertaining to CPNI,” stating that it was “not persuaded that any portion of section 222 indicates that Congress intended such a result.”¹⁷⁰ Yet again in 2007, the Commission wrote that “[e]very telecommunications carrier has a general duty pursuant to section 222(a) to protect the confidentiality of CPNI.”¹⁷¹

The fact that the Commission has only now — after 18 years — claimed to discover new authority within Section 222 over *all PII* held by all telecommunications carriers, rather than only CPNI, belies that novel statutory interpretation. As the Supreme Court has cautioned, “[w]hen an agency claims to discover in a long-extant statute an unheralded power to regulate a significant portion of the American economy, we typically greet its announcement with a measure of skepticism. We expect Congress to speak clearly if it wishes to assign to an agency decisions of vast economic and political significance.”¹⁷²

Even aside from its novelty, the Commission’s attempt to read the phrase “protect the confidentiality of proprietary information of . . . customers” in Section 222(a) to authorize the Commission to adopt extensive regulations governing carriers’ use and protection of “personally identifiable information” that is not CPNI fails for at least five reasons.

¹⁶⁹ Second Report and Order and Further Notice of Proposed Rulemaking, *Implementation of the Telecommunications Act of 1996*, 13 FCC Rcd 8061, ¶ 2 (1998).

¹⁷⁰ Order on Reconsideration and Petitions for Forbearance, *Implementation of the Telecommunications Act of 1996*, 14 FCC Rcd 14409, ¶ 147 (1999).

¹⁷¹ Report and Order and Further Notice of Proposed Rulemaking, *Implementation of the Telecommunications Act of 1996*, 22 FCC Rcd 6927, ¶ 6 (2007); *see also id.* ¶ 1 (“Section 222 of the Communications Act requires telecommunications carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure.”).

¹⁷² *Utility Air Regulatory Grp. v. EPA*, 134 S. Ct. 2427, 2444 (2014) (citation and internal quotation marks omitted).

First, reading Section 222(a) to impose limitations on carriers' use of PII that is not also CPNI would require rewriting other parts of Section 222, which the Commission lacks the power to do. For example, Section 222(d) permits a telecommunications carrier to use and disclose CPNI in various circumstances notwithstanding the limitations in Section 222(c), such as to bill customers. And Section 222(e) creates an exception from subsections (b), (c), and (d) for the publication of subscriber list information. Customer bills and subscriber lists undisputedly use information that the Commission now proposes to classify as PII subject to restrictions on use found in Section 222(a). Yet neither Section 222(d) nor Section 222(e) contains an exception from the requirements of Section 222(a).

The NPRM recognizes this problem, but, rather than concluding that its novel interpretation of Section 222(a) is internally inconsistent with other provisions of the statute, the Commission proposes to rewrite the statute. The Commission proposes (at ¶ 115) to “adopt the[] exceptions” in Section 222(d) “to the use or disclosure of all customer [proprietary information].” But the statute says no such thing. The Commission also seeks (at ¶ 64) to read out of the statute the exception in Section 222(e) for subscriber list information, noting that “today’s broadband providers do not publish directories of customer information” and so “there is no subscriber list information in the broadband context.” Even aside from the fact that nothing in the text of Section 222(e) permits the Commission to limit certain carriers’ right to publish subscriber lists, the Commission ignores that its reinterpretation of Section 222(a) would apply also to voice providers, which do publish subscriber lists that contain what the Commission now proposes to classify as protected PII. The Commission “has no power to ‘tailor’ legislation to bureaucratic policy goals by rewriting unambiguous statutory terms.”¹⁷³ The fact that the only

¹⁷³ *Utility Air*, 134 S. Ct. at 2445.

way to effectuate the Commission’s proposed reading of Section 222(a) is to rewrite other provisions of Section 222 demonstrates that the Commission’s reading is erroneous.

Second, Congress carefully crafted Section 222 to regulate CPNI. It precisely defined CPNI,¹⁷⁴ rejecting draft versions of the statute that included open-ended definitions for CPNI.¹⁷⁵ Congress also carefully identified the permissible uses of CPNI, choosing only to prohibit, with some exceptions, the unauthorized use of individually identifiable CPNI.¹⁷⁶ Despite Congress’s special focus on the uses of CPNI, the Commission claims that Congress simultaneously, in an introductory “In general” provision, granted it entirely unguided authority to adopt rules governing the use of PII that is not also CPNI. But “Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions — it does not, one might say, hide elephants in mouseholes.”¹⁷⁷ Given the care with which Congress addressed CPNI, if Congress had intended the Commission also to regulate PII (that is not also CPNI), it surely would have adopted specific provisions to address that additional customer information.

Third, when Congress intends to protect “personally identifiable information,” “it knows how to do so.”¹⁷⁸ Congress uses the term “personally identifiable information” when it intends to refer to PII; indeed, it has done so in the Communications Act itself and in an array of other federal statutes.¹⁷⁹ The fact that Congress did not use “personally identifiable information” in

¹⁷⁴ See 47 U.S.C. § 222(h)(1).

¹⁷⁵ See *supra* p. 55.

¹⁷⁶ See 47 U.S.C. § 222(c)(1), (d).

¹⁷⁷ *Whitman v. American Trucking Ass’ns, Inc.*, 531 U.S. 457, 468 (2001).

¹⁷⁸ *Dole Food Co. v. Patrickson*, 538 U.S. 468, 476 (2003).

¹⁷⁹ See 47 U.S.C. § 551 (Communications Act provision using the term “personally identifiable information” repeatedly); see also, e.g., 18 U.S.C. § 2710(b) (Video Privacy Protection Act of 1988); 20 U.S.C § 1232g (Family Educational Rights and Privacy Act of 1974).

the 1996 Act or in any amendment to the Act since 1996 is further confirmation that Section 222, as it applies to retail customers' information, is limited to CPNI.

Fourth, the fact that Section 222(a) refers to “proprietary information of . . . customers” and not “customer proprietary network information” is of no importance. Congress did not refer only to CPNI in Section 222(a) but also to proprietary information of other carriers and proprietary information of equipment manufacturers:

Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers

The absence of the word “network” from this general formulation is fully explained by the awkwardness of inserting that word into this general provision, particularly given Congress's failure elsewhere in the Act to use “proprietary information of . . . customers” to mean PII. Notably, even now the Commission does not suggest that Section 222(a) grants it unguided authority to impose additional obligations on carriers with respect to the proprietary information of other carriers or equipment manufacturers.

Fifth, in all events, Section 222(a) is far too thin a reed to authorize the entire regulatory apparatus the Commission proposes to erect for PII that is not CPNI. Section 222(a) requires only that carriers “protect the confidentiality” of information; it does not govern permissible *uses* of information. “Protecting” information does not include limiting a carrier's use of that information. “Protect” means to cover, shield, secure, or preserve something from injury, attack, or harm.¹⁸⁰ The remaining subsections of the statute, Sections 222(b) through (g), govern the

¹⁸⁰ See, e.g., *Protect*, *Webster's Third New International Dictionary* 1822 (2002) (“to cover or shield from that which would injure, destroy, or detrimentally affect: secure or preserve [usually] against attack, disintegration, encroachment, or harm”); *Protect*, *The American Heritage Dictionary of the English Language* 1416 (2011) (“1a. To keep from being damaged, attacked, stolen, or injured; guard. . . b. To keep from being subjected to difficulty or unpleasantness . . . c. To keep from being curtailed or exposed to risk . . .”).

permissible uses of information, and they specify the information they cover. The Commission suggests that the phrase “protect the confidentiality” of information implicitly contains the power to regulate its use towards only “expected purposes.”¹⁸¹ But, where Congress intended to restrict carriers’ use of information, it specifically chose the word “use,” “disclose,” or “provide.”¹⁸² The Supreme Court warns that one should not conclude that “differing language in the two subsections has the same meaning in each” because it is wrong to “presume to ascribe this difference to a simple mistake in draftsmanship.”¹⁸³ “Protect” and “use” are different words and must have different meanings.

2. *No Other Statutory Provision Authorizes the Proposed Rules*

The Commission identifies several other potential sources of authority for its proposed rules.¹⁸⁴ None authorizes the Commission to go beyond the limits in Section 222 and to adopt its proposed rules.

The provisions in Title II and Title III that the Commission cites in the NPRM — Sections 201, 202, 303, and 316 — are general provisions that speak broadly of reasonableness and the public interest.¹⁸⁵ “However inclusive may be the general language of a statute, it will not be held to apply to a matter specifically dealt with in another part of the same enactment. Specific terms prevail over the general in the same or another statute which otherwise might be

¹⁸¹ NPRM ¶ 300.

¹⁸² *See, e.g.*, 47 U.S.C. § 222(c)(1) (“use, disclose, or permit access to”), (e) (“shall provide”), (f) (“the use or disclosure”).

¹⁸³ *Russello v. United States*, 464 U.S. 16, 23 (1983).

¹⁸⁴ *See* NPRM ¶¶ 304-310.

¹⁸⁵ *See* 47 U.S.C. §§ 201(b), 202(a) (prohibiting “unjust or unreasonable” practices); *id.* § 303(b) (permitting the Commission to “[p]rescribe the nature of the service to be rendered by each class of licensed stations” as “public convenience, interest, or necessity requires”); *id.* § 316(a) (permitting the Commission to modify a “station license” if “such action will promote the public interest, convenience, and necessity”).

controlling.”¹⁸⁶ Because the Commission previously only regulated the use of CPNI by AT&T, the BOCs, and GTE,¹⁸⁷ Congress enacted a specific statute governing the protection and use of CPNI obtained by *any* telecommunications carrier from its customers: Section 222. Congress considered including a broad definition of CPNI in Section 222, but ultimately decided strictly to circumscribe the customer information it covered to the six categories listed in Section 222(h)(1).¹⁸⁸ Section 222 is “the sole and exclusive provision” governing the issue of customer information, and “it is not to be supplemented” by the more general provisions cited in the NPRM.¹⁸⁹ Moreover, the provisions of Title III the NPRM cites¹⁹⁰ — including Sections 303(b), 303(r), and 316¹⁹¹ — govern the Commission’s power over the technical requirements for radio broadcast stations. In particular, Section 303 provides the Commission with authority to classify radio stations and regulate their frequencies, location, transmissions, and similar technical matters. Nothing in these provisions grants the Commission a broad mandate to enact a new privacy regime untethered to the specific provisions of Section 222.¹⁹²

¹⁸⁶ *Fourco Glass Co. v. Transmirra Prods. Corp.*, 353 U.S. 222, 228-29 (1957) (internal quotation marks and alteration omitted).

¹⁸⁷ *See supra* p. 54.

¹⁸⁸ *See supra* p. 55.

¹⁸⁹ *Fourco Glass*, 353 U.S. at 229. The Commission seeks comment (at ¶ 306) on the extent to which it can adopt Federal Trade Commission precedents under Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibiting unfair methods of competition and unfair or deceptive acts or practices. The FTC Act does not contain a specific provision on data protection and use similar to Section 222. Therefore, the FTC may regulate data protection and use under its broad statutory authority. *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3d Cir. 2015). The Commission may not.

¹⁹⁰ *See* NPRM ¶ 310.

¹⁹¹ 47 U.S.C. §§ 303(b), 303(r), 316.

¹⁹² The Commission’s proposed rules are different from the data-roaming rule the D.C. Circuit upheld in *Cellco Partnership v. FCC*, 700 F.3d 534 (D.C. Cir. 2012). In that case, the court concluded that the data-roaming rule was consistent with Section 303(b) because it prescribed the nature of the service provided to the customer — it “define[d] the form mobile-

Section 705 of the Communications Act¹⁹³ prohibits only the unauthorized disclosure of the *contents* of communications, stating that “no person . . . transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof” except to an authorized person.¹⁹⁴ Section 705 is thus an anti-wiretapping statute — indeed, it expressly cross-references the Wiretap Act — and is not a general privacy provision. Moreover, none of the items the Commission proposes to classify as PII in the NPRM includes the contents of communications.¹⁹⁵

Finally, Section 706 of the 1996 Act¹⁹⁶ cannot support the proposed regulations. The Commission theorizes that the proposed regulations “have the potential to increase customer confidence in [broadband Internet access service] providers’ practices, thereby boosting confidence in and therefore use of broadband services.”¹⁹⁷ But there is no evidence that such a theory is true. Consumers today do not view privacy as a reason not to purchase broadband Internet access service.¹⁹⁸

internet service must take for those who seek a license to offer it.” *Id.* at 543. The Commission’s proposed rules here do not prescribe the service that broadband providers are authorized to offer — instead, they purport to regulate how providers may use and disclose customer information that they have obtained from rendering the service.

¹⁹³ 47 U.S.C. § 605.

¹⁹⁴ *Id.* § 605(a).

¹⁹⁵ See NPRM ¶ 62,

¹⁹⁶ 47 U.S.C. § 1302. Verizon continues to maintain that Section 706 is not an affirmative grant of authority to the Commission.

¹⁹⁷ NPRM ¶ 309.

¹⁹⁸ See National Telecomms. & Info. Admin., U.S. Dep’t of Commerce, *Exploring the Digital Nation: Embracing the Mobile Internet* 26 (Oct. 2014) (only 1% of households without Internet access identified privacy or security concerns as a primary reason for not using the Internet at home), available at https://www.ntia.doc.gov/files/ntia/publications/exploring_the_digital_nation_embracing_the_mobile_internet_10162014.pdf.

E. The Commission Should Allow Business Customers To Negotiate Alternative Arrangements and Customer Information To Be Used To Route Traffic

In addition to the problems already discussed, the Commission’s proposed rules will lead to an additional set of discrete issues and impose burdens on customers that cannot be justified:

1. The Commission Should Allow Business Customers To Negotiate Specific Privacy Terms

Because the Commission did not reclassify broadband services sold to enterprise and government customers, the privacy rules proposed in the NPRM do not apply to such services. But the line between enterprise and small-business customers is unsustainable, and the Commission’s proposed rules threaten to interfere with the contractual arrangements that broadband providers have reached with their small-business and E-rate customers (*i.e.*, schools and libraries). These businesses need the flexibility to negotiate customer-specific terms for the handling of their own customer information. Under the Commission’s existing CPNI rules, “[t]elecommunications carriers may bind themselves contractually to authentication regimes other than those described in this section for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses the carriers’ protection of CPNI.”¹⁹⁹ The Commission sensibly recognized that the privacy rules that apply to consumers may not make sense for businesses. Indeed, many businesses may want their CPNI used in different ways than a typical consumer. But the Commission’s proposed rules make no allowance for such contracts.

The Commission should allow telecommunications service providers to reach agreements with businesses regarding privacy terms other than those outlined in the Commission’s rules, as long as such terms are specifically addressed in the contract between the parties. Given the

¹⁹⁹ 47 C.F.R. § 64.2010(g).

sophistication of these customers and the fact that these customers will have the opportunity to negotiate specific terms of service with their providers, telecommunications service providers should be accorded the ability to come up with alternative arrangements for how best to handle business customer information.

2. *As in the Voice Context, Broadband Providers Must Be Allowed To Share Customer Information To Transmit and Route Traffic and for Network Maintenance*

Telecommunications service providers are currently permitted to use, disclose, or permit access to individually identifiable CPNI to a third party without customer approval when it is used, disclosed, or accessed in connection with the provision of a telecommunications service from which providers received the information, or a service necessary to or used in the provision of the service from which providers received the information.²⁰⁰ The provision of broadband service includes and requires the ability to troubleshoot and resolve issues with the service; to maintain the safety, security, speed, and operability of the service; and to manage the broadband network.²⁰¹ The Commission should take the opportunity to affirm that broadband providers may access and transmit customer information to third parties to fulfill these obligations.²⁰² Such disclosures should not be considered a breach under the privacy framework, and broadband providers should not be held liable for any misuse of the data by the recipient of the customer information or for failing to obtain contractual commitments from the recipient.

²⁰⁰ See 47 U.S.C. § 222(c)(1).

²⁰¹ See *Open Internet Order* ¶ 215.

²⁰² See NPRM ¶ 112.

III. THE INFLEXIBLE DATA-SECURITY AND BREACH-NOTIFICATION PROPOSALS ARE FLAWED AND COUNTERPRODUCTIVE

A. Rigid Data-Security Requirements Would Be Ineffective and Unreasonable

When it comes to data security, the Obama Administration has highlighted the need for a “flexible and evolving approach to changing technologies and markets.”²⁰³ Verizon agrees.

Thus, the Commission’s standards for data security should be flexible, because the Internet — and security threats on the Internet — are constantly changing.

Notably, and in keeping with the White House’s 2012 Privacy Report, the FTC follows a flexible approach that requires all Internet companies to practice reasonable data security. The FTC recognizes that data-security measures are fundamentally context-dependent: “[A] company’s data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.”²⁰⁴ This context-driven approach ensures data is appropriately protected while a one-size-fits-all approach would inevitably force regulated businesses to do too much or too little in individual circumstances.

Verizon supports reasonable data-security procedures for broadband providers’ customer information. These procedures, as the FTC has found, should vary based on providers’ different circumstances — *e.g.*, different network technologies, data sets, size and complexity of the business — as well as be allowed to evolve over time.²⁰⁵ In the world of data security, if

²⁰³ White House 2012 Privacy Report at 29.

²⁰⁴ FTC, Data Security, <https://www.ftc.gov/datasecurity>.

²⁰⁵ Plaintiff’s Response in Opp. to Wyndham Hotels and Resorts’ Mot. To Dismiss at 12, *FTC v. Wyndham Worldwide Corp., et al.*, No. 2:12-cv-01365-PHX-PGR, ECF No. 45 (D. Ariz. filed Oct. 1, 2012) (“[I]ndustries and businesses have a variety of network structures that store or transfer different types of data, and reasonable network security will reflect the likelihood that such information will be targeted and, if so, the likely methods of attack.”).

everything is deemed critical, nothing can be treated as critical. Thus, prescriptive data-security regulations that do not take these factors into account will only harm consumers by creating a one-size-fits-none approach that will impose strict requirements on non-sensitive data that has a very low risk of attack, ultimately requiring providers to divert limited resources away from more aggressively protecting more sensitive systems data.

Prescriptive data-security rules also could undermine the significant work that has gone into improving data security across the entire Internet ecosystem through several voluntary, collaborative multi-stakeholder processes. Those processes have resulted in data-security improvements across the board and led to the development of cybersecurity best practices, such as the NIST Cybersecurity Framework, that companies can work towards. Imposing prescriptive regulations at this point, however, could jeopardize companies' ability and willingness to participate in such efforts in the future.

If providers implement reasonable data-security procedures, they should not be held strictly liable if those procedures fail in particular situations. Data-security procedures are designed to minimize the risk of an attack. Even the best procedures, however, cannot completely eliminate that risk. On the contrary, a company may implement state-of-the-art technologies and still be the victim of an attack. Fraudsters' tactics are constantly evolving and companies are constantly trying to stay ahead of them. A single attack thus is not — and should not be viewed as — indicative of a systemic problem with the company's data-security procedures or a violation of the Commission's rules. Rather, companies must be held to a reasonableness standard for data security, which as noted above should be dependent on the provider's circumstances.

Similarly, providers should not be held strictly liable for the actions of third parties in the data-security space.²⁰⁶ While customer data accessed by contractors should be protected, and telecommunications providers should be required contractually to obligate those contractors to protect customer data, third parties are a different matter. In addition, telecommunications providers already have every incentive appropriately to vet the third parties with whom they contract and to engage in appropriate oversight to ensure that contractual obligations are met. So long as telecommunications providers use reasonable measures based on the scope of the data collected, follow standard industry practices to protect the security of the data, and require contractors to use similar practices, they should not be held accountable for failures of their contractors to adhere to their contractual obligations.

In addition to these recommendations, Verizon also urges the Commission to adopt the following proposals:

- Account Change Notices. Telecommunications service providers should not be required to notify customers of “attempts to access customer [proprietary information].”²⁰⁷ Such a requirement would inevitably lead to over-notification and exhaust customers’ attention. As written, the proposed rule requires notification whenever a customer mistypes a password in an attempt to gain access to his or her account or when a hacker unsuccessfully attempts to access a customer account (or millions of customers’ accounts). Requiring notice every time there has been an “attempt to access customer [proprietary information]” is vastly overbroad and will not achieve the Commission’s goals.
- Record of Customer Notices. The Commission should not require broadband providers to preserve copies of every notice sent to a customer;²⁰⁸ instead, providers should preserve what is necessary to demonstrate compliance with these rules.
- Address Definition. Verizon urges the Commission to allow broadband providers to send notifications to the customer that the provider “reasonably believes” to be most appropriate for contacting the customer. The Commission’s proposal requires broadband

²⁰⁶ See NPRM ¶ 211.

²⁰⁷ Proposed § 64.7005(a)(5); see also NPRM ¶ 201.

²⁰⁸ See NPRM ¶ 149.

providers to send written notice of a data breach “to the postal address of the customer *provided by the customer for contacting that customer.*”²⁰⁹ This requirement, however, lacks flexibility and prevents companies from developing creative ways to reach a customer. For example, some industries are providing notice via secure mailboxes in the customer’s online account. The objective should be to notify the customer in a manner reasonably likely to reach the customer. The Commission should not prescribe methods that may become outdated and less secure.

B. The Proposed Breach-Notification Requirements Are Inflexible and Burdensome

Verizon urges the Commission to adopt a reasonable, flexible framework for data-breach notifications that will provide consumers with the information they need about potentially harmful breaches without over-notifying them. To meet this goal, the Commission should require telecommunications service providers to notify customers of instances in which a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed individually identifiable CPNI and where such use, disclosure, or access is likely to cause consumer harm. In addition to striking the right balance between notification and over-notification, this approach has the added benefit of establishing uniform data-breach notification rules for all participants in the Internet ecosystem, so that customers can rely upon consistent, meaningful disclosures.

The Commission’s proposed rules, however, ignore this balance and instead would require telecommunications service providers to inundate their customers with notifications of breaches that will have no impact on customers. For example, the Commission’s proposed rule requires a broadband provider to provide notice of *any instance* when any customer data — not just CPNI — is inadvertently accessed by any person, regardless of materiality or whether any harm to the customer could result. That is unprecedented and extraordinarily broad. If a

²⁰⁹ Proposed § 64.7006(a)(1)(i) (emphasis added).

customer service representative accidentally mistypes an account number and thereby accesses the wrong account for an instant, the proposed rule might require that a customer notice be sent.

While the Commission acknowledges the harms of “notice fatigue,”²¹⁰ the inevitable result of the Commission’s proposal is that customers will receive notifications that they do not care about and that create unnecessary confusion and anxiety, such that customers could stop paying attention to notices altogether and miss those that might actually be important.

Meanwhile, the provider responsible for these excessive breach notifications will risk losing the customer’s trust for no good reason: for sending notifications when there has been no harm (or even risk of harm) to the customer’s privacy interests. This is particularly troubling because the Commission’s data-breach rules would apply only to telecommunications service providers, which means that other players in the Internet ecosystem — including social networking sites, search engines, and operating system and app developers — would be under no obligation to send similar notices in such innocuous circumstances. Because of this irregularity, customers would receive inconsistent breach notifications depending on the happenstance of which entity held their data. This cannot be the result the Commission intended. Verizon therefore urges the Commission to limit the requirement to provide customer notification to those breaches of customer information that have the potential to cause actual harm to the customer’s privacy interests.

This over-notification problem is exacerbated by the timeline that the Commission has proposed.²¹¹ In a typical breach situation, Verizon notifies the customer as soon as possible and in accordance with legal requirements, but 10 days is not a reasonable timeframe for all

²¹⁰ NPRM ¶ 23; *id.* ¶ 202 (“How can we ensure that our proposal does not result in customer ‘notice fatigue,’ lessening the usefulness of notices?”).

²¹¹ *See id.* ¶ 236.

breaches. State requirements are typically far more flexible, ranging from 30 to 90 days.²¹² For serious and complicated breaches, 10 days is just not enough time. In addition, for minor breaches, a 10-day notification period will require resources that could be spent responding to and notifying consumers of significant breaches to be diverted. Thus, the Commission should allow broadband providers some flexibility in the timing of customer breach notifications.

Finally, according to the Commission's proposal, whenever a telecommunications service provider discovers a breach that they reasonably believe has affected at least 5,000 customers, they must make separate reports to the Commission, on the one hand, and to the FBI and the Secret Service, on the other hand.²¹³ There is no reason to require two separate reports and forms. It should be sufficient, whenever the 5,000-customer threshold is met, for the provider to submit a single form to the Government. The requirement to submit two separate forms is both burdensome and duplicative. Moreover, the broadband provider should not have to waste time filling out duplicative government paperwork when the priority should be to fix the problem and notify its customers.

IV. A PROHIBITION ON ARBITRATION WOULD BE UNLAWFUL AND UNNECESSARY

The Commission should not adopt its proposal to prohibit broadband providers from including arbitration clauses in their customer contracts. Such a proposal would be unlawful and contrary to the public interest.

²¹² See Perkins Coie LLP, Security Breach Notification Chart (rev. Jan. 2016), <https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html> (last visited May 26, 2016).

²¹³ See NPRM ¶ 246; see also Proposed § 64.7006(c).

A. The Commission May Not Restrict Arbitration in Contravention of the Federal Arbitration Act

A “basic tenet” of administrative law is that, “‘in order to be valid,’” regulations must be “‘consistent’” with federal statutes.²¹⁴ They must not “exceed[]” the agency’s “statutory authority” conferred by the law under which the regulations are promulgated,²¹⁵ and they must also be consonant with “other Acts” of Congress that speak “to the topic at hand.”²¹⁶ The Commission’s proposal to ban broadband providers from including arbitration clauses in customer contracts would be invalid because it finds no support in the Communications Act and flatly contradicts the Federal Arbitration Act (“FAA”), 9 U.S.C. § 1 *et seq.*

The proposal exceeds the Commission’s authority under the Communications Act. The Commission has not cited any precedent that would support an agency’s attempt to promulgate regulations specifying the manner in which private parties must resolve disputes that are not adjudicated by the agency itself, and the Communications Act does not grant such authority. The Commission purports to rely principally on its authority under Section 222 of the Act.²¹⁷ But that section says nothing about dispute resolution. The proposed restriction on arbitration would not be a valid exercise of the Commission’s general authority to “prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions” of the Communications Act.²¹⁸ The Commission cites no “provision[]” it believes the restriction on arbitration would be “necessary” to “carry out.” The proposed arbitration restriction would not

²¹⁴ *Decker v. Northwest Env’tl Def. Ctr.*, 133 S. Ct. 1326, 1334 (2013) (citation omitted).

²¹⁵ *Heckler v. Campbell*, 461 U.S. 458, 466 (1983).

²¹⁶ *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000).

²¹⁷ See NPRM ¶ 294.

²¹⁸ 47 U.S.C. § 201(b).

advance the Commission’s interest in “protect[ing]” consumers’ “private information.”²¹⁹

Customers retain the ability to vindicate these interests through arbitration or, as appropriate, to bring such matters to the Commission’s attention.²²⁰ The Commission itself, moreover, retains the ability to investigate alleged privacy violations and enforce privacy regulations.

The proposal would also conflict with the FAA, which provides in relevant part that any “written provision in any . . . contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction . . . shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract.”²²¹ The FAA “establishes ‘a liberal federal policy favoring arbitration agreements,’” and it “requires courts to enforce agreements to arbitrate according to their terms.”²²² This rule extends to consumer contracts in the telecommunications setting,²²³ and it also extends to claims arising under federal statutes.²²⁴ The FAA’s protection for arbitration agreements thus applies to agreements between broadband providers and their customers to arbitrate disputes, including disputes arising under the Communications Act.

The Commission’s proposal is closely analogous to the California rule the Court invalidated in *Concepcion*. That rule, articulated by the California Supreme Court in *Discover*

²¹⁹ NPRM ¶ 274.

²²⁰ “You can also bring any issues you may have to the attention of federal, state, or local government agencies, and if the law allows, they can seek relief against us for you.” Verizon Wireless, “Customer Agreement,” <http://www.verizonwireless.com/b2c/support/customer-agreement>.

²²¹ 9 U.S.C. § 2.

²²² *CompuCredit Corp. v. Greenwood*, 132 S. Ct. 665, 669 (2012) (quoting *Moses H. Cone Mem’l Hosp. v. Mercury Constr. Corp.*, 460 U.S. 1, 24 (1983)).

²²³ See *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 346-47 (2011).

²²⁴ *CompuCredit*, 132 S. Ct. at 673; *American Express Co. v. Italian Colors Restaurant*, 133 S. Ct. 2304, 2309 (2013)

Bank v. Superior Court, 113 P.3d 1100 (Cal. 2005), precluded arbitration clauses in consumer contracts that waived the consumer’s right to bring a class or collective (as opposed to individual) arbitration proceeding.²²⁵ The U.S. Supreme Court reasoned that the FAA’s “overarching purpose” was “to ensure the enforcement of arbitration agreements according to their terms so as to facilitate streamlined proceedings,” and “[r]equiring the availability of classwide arbitration interferes with fundamental attributes of arbitration and thus creates a scheme inconsistent with the FAA.”²²⁶

Here, the Commission proposes to replace the “judicial hostility to arbitration” that the FAA was intended to overcome²²⁷ with administrative hostility to arbitration that is similarly contrary to the policy judgment made by Congress. The Commission cites media commentary arguing that, as the Commission puts it, “arbitration proceedings lack transparency, are often biased against consumers, and do not abide by traditional due process procedures.”²²⁸ These opinions bear no resemblance to Verizon’s arbitration practices.²²⁹ More fundamentally, however, the Commission’s views on that question are inapposite, because *Congress has already made the applicable policy judgment*. It has adopted a “‘liberal federal policy favoring arbitration,’” which precludes other governmental bodies from “requir[ing] a procedure that is inconsistent with the FAA,” even if they view it as “desirable” from a policy standpoint.²³⁰ An

²²⁵ See *Concepcion*, 563 U.S. at 340 (citing *Discover Bank*, 113 P.3d at 1110).

²²⁶ *Id.* at 344.

²²⁷ *Id.* at 339.

²²⁸ NPRM ¶ 273 n.429; see also *id.* ¶ 274 & n.431.

²²⁹ See *infra* pp. 79-80.

²³⁰ *Concepcion*, 563 U.S. at 339, 351 (quoting *Moses H. Cone Mem’l Hosp.*, 460 U.S. at 24); see also *Ivey v. D.R. Horton, Inc.*, No. 3:08-cv-598-CMC, 2008 WL 2717863, at *2 (D.S.C. July 10, 2008) (“[T]he ‘liberal federal policy favoring arbitration agreements’ reflects Congress’

agency may not interpret its governing statute in a manner that would conflict with the language or policy expressed in another federal statute.²³¹ The FAA’s text and policy in favor of private arbitration agreements control unless “the FAA’s mandate has been ‘overridden by a contrary congressional command.’”²³² Only federal statutes that *expressly* preclude or impose conditions on arbitration clauses, or that *expressly* authorize agencies to do so by regulation, meet this standard.²³³ In this instance, the Commission can point to no such statute or delegation of authority to contravene the FAA. Indeed, the Act evinces no congressional intent to override the FAA, and, were the Commission to conclude otherwise, its reasoning would not receive deference and would not survive a judicial challenge.

The cause of action created by the Communications Act does not authorize the Commission to ban private arbitration agreements. In *CompuCredit*, the Court rejected an argument that the Credit Repair Organization Act somehow precluded an agreement to arbitrate when it provided consumers “‘a right to sue a credit repair organization that violates the Credit Repair Organization Act’” and declared “‘void’” any “‘waiver by any consumer of any

perspective on the fairness and efficiency of arbitration as a process for dispute resolution.”) (quoting *Moses H. Cone Mem’l Hosp.*, 460 U.S. at 24).

²³¹ See *Brown & Williamson*, 529 U.S. at 157 (holding that the FDA could not interpret its statute, giving the agency broad discretion to regulate “drugs,” to apply to tobacco, when such a construction would be inconsistent with the presumption reflected in other federal statutes that tobacco would not be so regulated); see also *Hoffman Plastic Compounds, Inc. v. NLRB*, 535 U.S. 137, 144 (2002) (“[W]e have accordingly never deferred to the Board’s remedial preferences where such preferences potentially trench upon federal statutes and policies unrelated to the [National Labor Relations Act (“NLRA”)].”).

²³² *Italian Colors*, 133 S. Ct. at 2309 (quoting *CompuCredit*, 132 S. Ct. at 668-69).

²³³ See *CompuCredit*, 132 S. Ct. at 672; see also, e.g., 7 U.S.C. § 26(n)(2) (“No predispute arbitration agreement shall be valid or enforceable, if the agreement requires arbitration of a dispute arising under this section.”); 15 U.S.C. § 1226(a)(2) (“Notwithstanding any other provision of law, whenever a motor vehicle franchise contract provides for the use of arbitration to resolve a controversy arising out of or relating to such contract, arbitration may be used to settle such controversy only if after such controversy arises all parties to such controversy consent in writing to use arbitration to settle such controversy.”).

protection provided by or any right of the consumer under this subchapter.’”²³⁴ The Court held that, “[i]f the mere formulation of the cause of action in this standard fashion were sufficient to establish the ‘contrary congressional command’ overriding the FAA, valid arbitration agreements covering federal causes of action would be rare indeed. But that is not the law.”²³⁵ The same conclusion holds here: there simply is no provision in the Communications Act that authorizes the Commission to contravene the pro-arbitration text and policy of the FAA.²³⁶

B. Prohibiting Arbitration Would Harm Consumers

In addition to being unlawful, the proposal to ban mandatory arbitration clauses would be contrary to the public interest. The Commission has expressed its “agree[ment] with the

²³⁴ 132 S. Ct. at 669 (quoting 15 U.S.C. §§ 1679c(a), 1679f(a)).

²³⁵ *Id.* at 670 (citation omitted). *See also Gilmer v. Interstate/Johnson Lane Corp.*, 500 U.S. 20, 29 (1991) (rejecting argument that Age Discrimination in Employment Act of 1967 precluded agreement to arbitrate, reasoning that “Congress . . . did not explicitly preclude arbitration or other nonjudicial resolution of claims”); *Shearson/American Express, Inc. v. McMahon*, 482 U.S. 220, 228, 238 (1987) (same conclusion for claims arising under the Securities Exchange Act of 1934 and the Racketeer Influenced and Corrupt Organizations Act); *Mitsubishi Motors Corp. v. Soler Chrysler-Plymouth, Inc.*, 473 U.S. 614, 628-29 (1985) (same conclusion for federal antitrust claims).

²³⁶ Whether the statutory text authorizes an agency’s prohibition of arbitration clauses containing a class-action waiver may be less clear under other federal statutes. *Compare D.R. Horton, Inc. v. NLRB*, 737 F.3d 344, 360 (5th Cir. 2013) (holding that the NLRA “should not be understood to contain a congressional command overriding application of the FAA,” rejecting the Board’s argument that “the general thrust of the NLRA — how it operates, its goal of equalizing bargaining power” reflected the required indication of a congressional desire to restrict mandatory arbitration clauses); *Owen v. Bristol Care, Inc.*, 702 F.3d 1050, 1053 (8th Cir. 2013) (rejecting argument that there is inherent conflict between the NLRA and the FAA); *Sutherland v. Ernst & Young LLP*, 726 F.3d 290, 297 n.8 (2d Cir. 2013) (per curiam) (same); *and Richards v. Ernst & Young, LLP*, 744 F.3d 1072, 1075 n.3 (9th Cir. 2013) (per curiam) (same), *cert. denied*, 135 S. Ct. 355 (2014), *with Lewis v. Epic Sys. Corp.*, No. 15-2997, slip op. 3, 22 (7th Cir. May 26, 2016) (to be reported in F.3d) (disagreeing with three other Circuits and holding that the NLRA’s express protection of employees’ right to engage in “concerted activities for the purpose of collective bargaining or other mutual aid or protection” invalidates an employee’s agreement to a mandatory arbitration provision containing a class-action waiver) (quoting 29 U.S.C. § 157). Regardless of the ultimate resolution of this question under the NLRA, the Communications Act contains no comparable provision that provides any basis for the Commission’s effort to prohibit mandatory arbitration provisions.

observation that ‘mandatory arbitration, in particular, may more frequently benefit the party with more resources and more understanding of the dispute procedure, and therefore should not be adopted.’²³⁷ The evidence does not support that conclusion, as Verizon’s consumer-friendly arbitration procedure demonstrates.

First, the evidence belies the Commission’s suggestion that arbitration disadvantages consumers. Multiple studies have found that consumers obtain relief in arbitration at rates higher than they do in court.²³⁸

For instance, a 2010 study of claims filed with the American Arbitration Association (“AAA”) found that consumers win relief 53.3% of the time.²³⁹ Studies of arbitrations conducted by the National Arbitration Forum reflect similar results.²⁴⁰ By contrast, the best available estimates are that plaintiffs in state and federal court win some form of relief approximately 50% of the time.²⁴¹ In class actions, the success rate for plaintiffs is even lower: virtually none of

²³⁷ NPRM ¶ 274 (quoting *Open Internet Order* ¶ 267).

²³⁸ See Peter B. Rutledge, *Whither Arbitration?*, 6 Geo. J.L. & Pub. Pol’y 549, 560 (2008) (analyzing multiple studies and finding that “raw win rates, comparative win rates, comparative recoveries, and comparative recoveries relative to amounts claimed . . . do not support the claim that consumers and employees achieve inferior results in arbitration compared to litigation”); David Sherwyn et al., *Assessing the Case for Employment Arbitration: A New Path for Empirical Research*, 57 Stan. L. Rev. 1557, 1567 (2005) (“What seems clear from the results of these studies is that the assertions of many arbitration critics were either overstated or simply wrong.”).

²³⁹ See Christopher R. Drahozal & Samantha Zyontz, *An Empirical Study of AAA Consumer Arbitrations*, 25 Ohio St. J. on Disp. Resol. 843, 845-46, 897 (2010).

²⁴⁰ See Mark Fellows, *The Same Result As In Court, More Efficiently: Comparing Arbitration And Court Litigation Outcomes*, Metropolitan Corporate Counsel 32 (July 2006) (showing that consumers prevailed in 65.5% of consumer-initiated cases that reached decision), available at <http://www.metrocorp counsel.com/pdf/2006/July/32.pdf>; Mary Batchner et al., *The Ernst & Young Study – Outcomes of Arbitration: An Empirical Study of Consumer Lending Cases* 6 (2004) (showing that consumers prevailed in 53 of 97 consumer-initiated cases that reached decision).

²⁴¹ See Theodore Eisenberg et al., *Litigation Outcomes in State and Federal Courts: A Statistical Portrait*, 19 Seattle U. L. Rev. 433, 437 (1996).

these cases are tried to judgment in the plaintiffs' favor, and only about one-third result in a settlement on a class-wide basis.²⁴² In short, based on the available evidence, "it cannot be said that mandatory arbitration in actual practice is detrimental" to claimants.²⁴³

Consumers who pursue arbitration can and do recover significant sums. The average amount recovered by prevailing consumer claimants in the AAA study was \$19,255, and the median amount was \$5,000.²⁴⁴ These figures translate to between 41.6% and 72.7% of the amount claimed, depending on the size of the claim.²⁴⁵ Claimants also frequently recover attorney's fees: prevailing claimants sought fees in a majority of cases, and the arbitrator awarded fees in 63.1% of the cases in which they were sought, with an average award of more than \$14,000.²⁴⁶ Indeed, in the seminal *Concepcion* case, the Supreme Court, the Ninth Circuit, and the district court all agreed that the arbitration scheme at issue was "sufficient to provide incentive for the individual prosecution of meritorious claims that are not immediately settled" and that it was *more* plaintiff-friendly than a class action in court.²⁴⁷

Second, there is no evidence to support the Commission's suggestion that consumers are disadvantaged in arbitration relative to repeat-player defendants. The AAA study found no statistically significant difference in repeat-player cases, with consumers prevailing in 51.8% of cases against such parties, roughly comparable to the success rate in cases against non-repeat-

²⁴² See Letter from David Hirschmann & Lisa A. Rickard, U.S. Chamber of Commerce, to Monica Jackson, Consumer Financial Protection Bureau, at 46-47 (Dec. 11, 2013) ("Chamber of Commerce Letter"), http://www.instituteforlegalreform.com/uploads/sites/1/2013_12.11_CFPB_-_arbitration_cover_letter.pdf.

²⁴³ Theodore J. St. Antoine, *Mandatory Arbitration: Why It's Better Than It Looks*, 41 U. Mich. J.L. Reform 783, 795-96 (2008).

²⁴⁴ See Drahozal & Zyontz, 25 Ohio St. J. on Disp. Resol. at 899.

²⁴⁵ See *id.* at 900.

²⁴⁶ See *id.* at 902.

²⁴⁷ 563 U.S. at 352.

player parties.²⁴⁸ Where consumer claimants do prevail on their claims, “they are awarded on average an almost identical percent of the amount claimed” against repeat-player parties (52.4%) as against non-repeat-player parties (52%).²⁴⁹ In addition, courts can and do invalidate arbitration agreements with biased procedures for selecting the arbitrator or other problems in the arbitration process, which provides consumers with an additional layer of protection against a theoretical “repeat player” advantage.²⁵⁰

Third, arbitration is significantly less costly and time-consuming for consumers than litigation. The rules of the AAA cap consumer fees at \$200, with all remaining fees borne by the company.²⁵¹ Justice Ruth Bader Ginsburg has described the AAA’s rules as “models for fair cost and fee allocation.”²⁵² In AAA consumer cases seeking less than \$10,000, consumer claimants paid an average of \$96.²⁵³ Other studies have found that, for low-income claimants in particular, arbitration offers the prospect of dispute resolution at manageable cost and without the need to hire an attorney, which will prove impossible in many cases.²⁵⁴ Arbitration also is significantly faster than litigation in resolving claims. In the AAA study, the average time from filing to final

²⁴⁸ See Drahozal & Zyontz, 25 Ohio St. J. on Disp. Resol. at 909.

²⁴⁹ *Id.* at 912; see also Elizabeth Hill, *Due Process at Low Cost: An Empirical Study of Employment Arbitration Under the Auspices of the American Arbitration Association*, 18 Ohio St. J. on Disp. Resol. 777, 785-88 (2003) (noting absence of empirical evidence of “repeat player” effect).

²⁵⁰ See, e.g., *Chavarria v. Ralphs Grocery Co.*, 733 F.3d 916, 923-25 (9th Cir. 2013).

²⁵¹ See AAA, *Consumer Arbitration Rules: Costs of Arbitration (including AAA Administrative Fees)* at 1 (eff. Jan. 1, 2016), <https://www.adr.org/aaa/ShowPDF?doc=ADRSTAGE2026862>.

²⁵² *Green Tree Fin. Corp.-Alabama v. Randolph*, 531 U.S. 79, 95 (2000) (concurring in part and dissenting in part).

²⁵³ See Drahozal & Zyontz, 25 Ohio St. J. on Disp. Resol. at 845.

²⁵⁴ See *id.* at 903-07; Hill, 18 Ohio St. J. on Disp. Resol. at 802.

award was 6.9 months, compared to 25.2 months for cases in federal court that went to trial.²⁵⁵

The lower costs of arbitration and speedier pace of arbitration mean that, for many claimants, “it may in fact be their only feasible option.”²⁵⁶

Fourth, as a practical matter, much of the opposition to arbitration comes from plaintiff-side class-action attorneys. These attorneys are not disinterested parties: they have a direct financial stake in preserving class actions — which can net them millions of dollars of fees — as an alternative to arbitration. These class actions often deliver little or no tangible benefit to class members.²⁵⁷

Fifth, many companies — including Verizon — have voluntarily adopted a set of best practices designed to make arbitration even more consumer-friendly.²⁵⁸ For example, under Verizon’s customer agreement, disputes are resolved through arbitration conducted by either the AAA or the Better Business Bureau. Customers may initiate this arbitration simply by filing the required forms with the arbitrating agency. The company covers all arbitration fees, regardless of whether the customer or Verizon ultimately prevails. Customers are given a full and fair opportunity to present their arguments and evidence in writing, in person, or by phone. If the

²⁵⁵ See U.S. Courts, *Federal Judicial Caseload Statistics: March 31, 2015*, Table C-5, <http://www.uscourts.gov/statistics/table/c-5/federal-judicial-caseload-statistics/2015/03/31>; Drahozal & Zyontz, 25 Ohio St. J. on Disp. Resol. at 845.

²⁵⁶ St. Antoine, 41 U. Mich. J.L. Reform at 796.

²⁵⁷ See *Marek v. Lane*, 134 S. Ct. 8, 8-9 (2013) (Roberts, C.J., statement respecting denial of certiorari) (noting class-action settlement that awarded \$3 million in attorney’s fees with *no* financial recovery going to class members); see also, e.g., Martin H. Redish et al., *Cy Pres Relief and the Pathologies of the Modern Class Action: A Normative and Empirical Analysis*, 62 Fla. L. Rev. 617, 653-54 (2010) (noting the prevalence of “faux class actions, where the class action procedure is used primarily for the benefit of participants in the process other than the absent claimants”) (footnote omitted).

²⁵⁸ See Chamber of Commerce Letter at 30-38 (summarizing these efforts); *Concepcion*, 563 U.S. at 351-52 (noting consumer-friendly aspects of AT&T Mobility arbitration agreement at issue).

arbitrator awards the customer a lesser amount than Verizon offered in settlement, Verizon guarantees that the customer will receive a minimum of \$5,000 plus reasonable attorney's fees and costs.²⁵⁹

In light of this evidence and the consumer-friendly arbitration practices adopted at Verizon and in other industries, there simply is no basis for the Commission's conclusory and unsupported assertion that arbitration is unfair to consumers. The Commission's proposal to ban mandatory arbitration agreements between broadband providers and their customers is an unlawful solution in search of a nonexistent problem.

CONCLUSION

The Commission should withdraw the rules it has proposed in the NPRM or, alternatively, revise them to be consistent with the notice-and-choice framework that applies to all other participants in the Internet ecosystem.

²⁵⁹ See, e.g., Verizon Wireless, "Customer Agreement," available at <http://www.verizonwireless.com/b2c/support/customer-agreement>.

Respectfully submitted,

s/ Karen Zacharia

William H. Johnson
Of Counsel

Karen Zacharia
Catherine M. Hilke
Verizon
1300 I Street, N.W. – Suite 400 West
Washington, D.C. 20005
(202) 515-2438

Scott H. Angstreich
Geoffrey M. Klineberg
Kellogg, Huber, Hansen, Todd,
Evans & Figel, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
(202) 326-7900

Henry Weissmann
Munger Tolles & Olson, LLP
355 South Grand Avenue
35th Floor
Los Angeles, California 90071
(213) 683-9100

Counsel for Verizon

May 27, 2016

APPENDIX

SUMMARY OF VERIZON ADVERTISING PROGRAMS

This Appendix describes four Verizon advertising programs that use information collected from Verizon's wireless and wireline mass-market Internet service customers. Three are wireless programs (Relevant Mobile Advertising; Verizon Selects; and Business and Marketing Insights). The fourth is a wireline program (Relevant Online Advertising).

In all cases, Verizon gives customers the choice of whether to participate in these programs and provides clear and complete information to help customers decide what programs and services are best for them. Verizon does not share information that identifies its customers personally as part of any of these programs other than with vendors and partners who do work for Verizon. These vendors and partners are contractually obligated to protect the information and to use it only for the services they are providing to Verizon. And all of these programs are optional; that is, a customer's choice whether to participate does not affect the customer's ability to use Verizon services or the Verizon network.

1. **Relevant Mobile Advertising**

The Verizon Wireless Relevant Mobile Advertising ("RMA") program, which is part of the AOL Advertising Network,¹ helps make marketing that consumers see more personalized and useful. This program uses basic information about Verizon customers (including email or postal address) and demographic and interest information that Verizon purchases from third parties in order to help advertisers reach Verizon customers.

Information that Relevant Mobile Advertising Uses. The program uses relatively little information from Verizon's own records. The only Verizon customer information used in the program is email or postal address and certain information about a customer's products and

¹ In the fall of 2015, Verizon notified its customers that it was combining certain of its advertising programs with the AOL Advertising Network. [Att. 1]

Appendix to Comments of Verizon

services, such as the customer's device type. The RMA program also uses demographic and interest categories Verizon purchases from other companies such as gender, age range, and interests (*e.g.*, sports fan, frequent diner, or pet owner). This information may be combined with information the AOL Advertising Network collects when customers use AOL services and visit third-party websites where AOL provides advertising services (such as web browsing, app usage, and location, as well as information that AOL obtains from third-party partners and advertising). Information about the AOL Advertising Network can be found in the AOL privacy policy (<http://privacy.aol.com/privacy-policy/> and Att. 2).

For example, an automobile company may want to target ads to people who visited a dealership but did not buy a car. In this scenario, the company has the email addresses of the people it wants to receive ads when those individuals are browsing online or using an app. Verizon effectively serves as a “bridge” to the customer by delivering ads to the devices that correspond to the email addresses. The RMA program uses a third party to match the email addresses of people who visit the dealership and are Verizon customers in a way that protects the privacy of those email addresses.² As a result, the automobile company's ad can then be served to customers' devices that match the company's requirements. This type of targeted advertising is common across the Internet. As detailed below, customers may choose not to participate in this program by opting out. The RMA program is explained in Verizon's privacy policy (<http://www.verizon.com/about/privacy/full-privacy-policy> and Att. 3) and in additional FAQs that are posted online (<http://www.verizonwireless.com/support/mobile-ads-faqs/> and Att. 4).

² In this scenario, Verizon and the automobile company each provide a list of hashed email addresses to a third-party vendor. The vendor compares the lists and returns to Verizon a list of hashed emails where there is a match. Verizon then serves ads to customers who were on the “matched” list. Strict contractual provisions require the vendor to use the information only for this purpose, not to try to re-identify the individuals, and to protect and to secure the information it receives from Verizon.

Appendix to Comments of Verizon

The RMA program does not use information that Verizon Wireless has about the location of a mobile device, nor does it use information Verizon Wireless has about web browsing activity from program participants. However, ads served by AOL to Verizon customers that are in part based on information made available through the RMA program may also use location information that AOL independently collects or acquires from advertisers (for example, if an individual allows the MapQuest app to collect and use location information, that information may be used by AOL to help make advertising more relevant in accordance with the permission given by the app user). Additionally, AOL ads may use mobile and online web browsing information AOL independently collects.

How RMA Works. The Verizon Wireless RMA program uses online and device identifiers including AOL browser cookies, advertising IDs from Apple and Google, and one created by Verizon, known as a “Unique Identifier Header” or “UIDH.”

Unless the customer opts out of the RMA program (and has not opted in to the separate Verizon Selects program), a UIDH is included in the address information of Internet requests going to Verizon companies (including AOL).³ This address information is sometimes referred to as a “header.”⁴ The UIDH does not contain any personally identifiable data, and it does not broadcast individuals’ historical web browsing activity to advertisers or others. Separately, Verizon provides AOL with the marketing segments for each UIDH. Additional privacy protections are designed into the UIDH – for example, it changes automatically and frequently.

³ The UIDH is also included in the address information of Internet requests going to a small number of partners to help deliver services unrelated to advertising, such as authentication of devices on our network.

⁴ Header information is included in all web traffic and includes information such as the device type, preferred language, and content support so that the site receiving the request knows how to best display the site on the phone or other device that sends the request.

Appendix to Comments of Verizon

More information about the UIDH can be found at <http://www.verizonwireless.com/support/unique-identifier-header-faqs/> and in Attachment 5.

These identifiers are used to make Verizon's advertising programs better by, for example:

- Linking Verizon advertising program information to information AOL has, to provide more personalized advertising.
- Serving ads to customers in apps and web browsers that do not use common advertising identifiers.
- Helping to determine that different devices have the same user, so AOL can deliver better advertising in more places.
- Determining that an identifier fits into a marketing audience so that the device will receive particular relevant ads.
- Mitigating advertising fraud.
- Ad reporting, modeling, and attribution.

Customer Disclosures. Verizon provided existing customers with information about the RMA program and notified them of their ability to opt out prior to launching the program in the fall of 2011. In addition, Verizon provided existing customers with updated information when it combined the RMA program with the AOL Advertising Network in the fall of 2015. [Att. 1] Verizon informs new wireless customers about the program when they sign up for Verizon service. Customers can also obtain information on the RMA program at any time in the privacy policy (<http://www.verizon.com/about/privacy/full-privacy-policy> and Att. 3) or from the Verizon website's FAQs for the RMA program (<http://www.verizonwireless.com/support/mobile-ads-faqs/> and Att. 4).

Customer Choices. Customers may opt out of the RMA program at any time. Customers may opt out online at www.vzw.com/myprivacy on their device using the My Verizon application or by calling a toll-free number – (866) 211-0874.⁵ Customers may also opt out by

⁵ Verizon Wireless will stop inserting the UIDH after a customer opts out of the Relevant Mobile Advertising program. As explained in the Verizon Selects portion of this appendix, if a

calling a Customer Care Representative through the standard helpline (including *611 from any Verizon device). Verizon Wireless provides customers with an easy-to-use dashboard containing their privacy choices. [Att. 6] Customers also have choices about AOL's use of information it collects and uses for advertising purposes.⁶ The RMA program does not increase the number of ads that a customer sees, but instead helps to make sure those ads are better targeted to a customer's interests. As a result, customers will continue to receive ads even if they opt out of the RMA program.

2. Verizon Selects

Like RMA, Verizon Selects helps to make marketing to customers more personalized and useful. And, like RMA, Verizon Selects is part of the AOL Advertising Network. Verizon Selects uses the same information that is used in the RMA program plus additional, more sensitive information collected by Verizon. This more sensitive information includes websites customers visit, app and device feature usage, location information obtained by virtue of the customer using her broadband service, and Customer Propriety Network Information as that term is defined in the existing rules. For example, as part of the Verizon Selects program, a local golf course could have Verizon display its advertisement to customers who have visited golf-related websites and live in a particular zip code. This type of advertising is also common across the Internet.

Because this program uses more sensitive customer data, customers are enrolled in Verizon Selects only if they affirmatively opt in to the program.

customer chooses to participate in Verizon Selects, the UIDH will be present even if the customer has also opted out of the RMA program.

⁶ Customers also have choices about how AOL uses information for advertising purposes. [FAQ 9 at <http://www.verizonwireless.com/support/mobile-ads-faqs/> and Att. 4]

Appendix to Comments of Verizon

Information that Verizon Selects Uses. Verizon Selects uses:

- Websites visited, apps and features used, and device and advertising identifiers.
- Device location.
- Postal and email address.
- Customer's use of Verizon products and services and how they use them (such as data and calling features and use, Fios service options, equipment and device types). Some of this information is Customer Proprietary Network Information under existing FCC rules.
- Information Verizon obtains from other companies (such as gender, age range, interests, shopping preferences, and ad responses).

This information may be combined with information the AOL Advertising Network collects when customers use AOL Services and visit third-party websites where AOL provides advertising services (such as web browsing, app usage, and location), as well as information that AOL obtains from third-party partners and advertisers. This information is described in the AOL privacy policy. [<http://privacy.aol.com/privacy-policy/> and Att. 2]

How Verizon Selects Works. Verizon Selects generally operates in the same manner as the RMA program, only using more data to identify which customers should receive advertisements.

Like the RMA program, Verizon Selects uses the UIDH identifier. Verizon Selects use of the UIDH is identical to RMA's use of the identifier with one exception. When a customer provides opt-in consent, for example when a customer opts in to the Verizon Selects program, the customer consents that the UIDH may also be shared with partners who help provide advertising services. Although Verizon does not do this today, in the future, these Verizon partners will be authorized to use the UIDH only as part of Verizon and AOL services and not for their own separate uses.

Appendix to Comments of Verizon

Customer Disclosures. Verizon notifies customers about the Verizon Selects programs in different ways. For example, customers who are considering joining Verizon's Smart Rewards program are provided information about Verizon Selects. [Att. 7] In addition, in the past Verizon has offered customers signing up for the NFL Mobile app the opportunity to opt in to Verizon Selects. [Att. 8] The Verizon Selects participation agreement fully describes the program. [Att. 9] The Selects FAQs also contain detailed information about the program, explaining what customers agree to when they opt in, what information is used in the program, and how customers may change their selection. [<http://www.verizonwireless.com/support/verizon-selects-faqs/> and Att. 10]

Customer Choices. Customers may change their choice at any time by going to My Verizon. [Att. 11] Customers may also instruct Verizon to stop using past data it has collected about web browsing and location to direct ads in the Verizon Selects program. Verizon Wireless provides customers with an easy-to-use dashboard containing their privacy choices.

3. Business and Marketing Insights

Verizon's Business and Marketing Insights program uses certain customer information to create information that may be useful for advertisers or other businesses.

Information that Insights Uses. This program uses information about how customers use their mobile devices, including web browsing, apps and features customers use, and the location of their devices. It also uses certain information about customers' products and services (such as device type and amount of use) and information Verizon obtains from other companies (such as gender, age range, and interests).

How Insights Works. The Insights program combines the above-described information in a manner that does not identify customers individually and generates aggregated business and

Appendix to Comments of Verizon

marketing insights that Verizon may share with others for their uses. For example, Verizon might tell a website owner that 60% of the people who visited the site were women between the ages of 20-29.

Verizon may also share location information with others in a way that does not personally identify customers so that the third parties may produce their own aggregate reports. For example, the data Verizon provides could be combined with data provided by others to create a report on the number of individuals who take a particular highway during rush hour.

Customer Disclosures. Before initiating this program, Verizon provided existing customers with information about the program and notified them of their ability to opt out. Verizon provides new wireless customers a notice about the program when they sign up for Verizon service. Customers can also obtain information on the Insights program at any time in the privacy policy (<http://www.verizon.com/about/privacy/full-privacy-policy> and Att. 3) or through the FAQs (<http://www.verizonwireless.com/support/business-marketing-reports-faqs/> and Att. 12).

Customer Choices. Customers may opt out of the Insights program at any time. Customers may opt out online at www.vzw.com/myprivacy, on their device using the My Verizon application, or by calling a toll-free number – (866) 211-0874. Customers may also opt out by calling a Customer Care Representative through the standard helpline (including by dialing *611 from any Verizon Wireless device). Customers can also view and change their choices about participation by accessing the easy-to-use dashboard containing their privacy choices for this and other programs. [Att. 6]

4. Relevant Online Advertising

The Relevant Online Advertising program helps advertisers better reach Verizon's wireline Internet access customers. This program uses the same basic information that is used in the RMA program.

Information that Relevant Online Advertising Uses. This program uses customers' postal address and certain information about the Verizon products and services (such as broadband and video features) to which customers subscribe. The program also uses demographic and interest information that Verizon purchases from third parties.

How Relevant Online Advertising Works. As with the RMA program, the information used in the Relevant Online Advertising Program helps Verizon identify customers who an advertiser is trying to reach. For example, a local restaurant may want to advertise only to people who live within 10 miles and tend to be frequent diners. Verizon can help that advertiser reach that customer through an ad on a website without providing any information about the customer to an advertiser. For wireline broadband users, identifying the customer for this type of advertising is done based on the customer's IP address rather than Apple and Android advertising identifiers or a Verizon-created identifier such as the UIDH.

Customer Disclosures. Before initiating this program, Verizon provided existing customers with information about the program and notified them of their ability to opt out. Verizon provides new customers a notice about the program when they sign up for service. Customers can also obtain information about the Relevant Online Advertising program at any time in the privacy policy (<http://www.verizon.com/about/privacy/full-privacy-policy> and Att. 3) or online (<https://www.verizon.com/support/consumer/announcements/privacy-announcements/direct-digital-marketing> and Att. 13).

Appendix to Comments of Verizon

Customer Choices. Customers may opt out of the Relevant Online Advertising program at any time. To make this choice, customers may visit the My Verizon website. As with the RMA program, customers will continue to receive ads even if they opt out of the Relevant Online Advertising Program.

APPENDIX ATTACHMENT 1

Advertising Programs Privacy Notice - October 2015

AOL recently became part of Verizon. Verizon and AOL will work together to deliver services that are more personalized and useful to you.

The Verizon family of companies offers a wide and growing variety of free services, including The Huffington Post, MapQuest, and our new mobile video service, go90. Like many others online, these services are made possible by advertising. The best advertising is for something you might actually want, and that is what we want to give you.

To help make this happen, starting in November, we will combine Verizon's existing advertising programs—Relevant Mobile Advertising and Verizon Selects—into the AOL Advertising Network. The combination will help make the ads you see more valuable across the different devices and services you use.

What information do these advertising programs use?

The [Relevant Mobile Advertising program](#) uses your postal and email addresses, certain information about your Verizon products and services (such as device type), and information we obtain from other companies (such as gender, age range, and interests). The separate [Verizon Selects](#) program uses this same information plus additional information about your use of Verizon services including mobile Web browsing, app and feature usage and location of your device. The [AOL Advertising Network](#) uses information collected when you use AOL services and visit third-party websites where AOL provides advertising services (such as Web browsing, app usage, and location), as well as information that AOL obtains from third-party partners and advertisers.

We do not share information that identifies you personally as part of these programs other than with vendors and partners who do work for us. We require that these vendors and partners protect the information and use it only for the services they are providing us.

How do these advertising programs work?

These programs use online and device identifiers, including AOL browser cookies, ad IDs from Apple and Google, and one created by Verizon, known as a "Unique Identifier Header." When the Verizon and AOL programs are combined, this Verizon identifier will be inserted in certain Web traffic that is sent only to Verizon companies (including AOL) and to certain partners. These partners will be authorized to use the Verizon identifier only as part of Verizon and AOL services.

We will use these identifiers to help make our advertising programs better by, for example:

- Linking Verizon advertising program information to information AOL has, to provide more personalized advertising.
- Connecting app and web browsing activity so ads linked to your interests can appear in both.
- Helping to determine that different devices have the same user so AOL can deliver better advertising in more places.

Your choices

The privacy of our customers is important to us, and if you don't want to participate in these programs, you don't have to. You can opt out of Relevant Mobile Advertising by visiting [your privacy choices page in MyVerizon](#) or calling 1.866.211.0874. If you have previously opted out of Relevant Mobile Advertising, you do not need to opt out again. You are only part of Verizon Selects if you have joined or choose to opt in to Verizon Selects in the future. You can see your participation status and makes changes at [your privacy choices page in MyVerizon](#).

You also have [choices about how AOL uses information](#) for advertising purposes. Please note that using browser controls such as clearing cookies on your devices or clearing your browser history is not an effective way to opt out of the Verizon or AOL advertising programs.

Additional information

[Relevant Mobile Advertising FAQs](#)

See FAQs related to relevant mobile advertising.

[Verizon Selects FAQs](#)

Learn what Verizon Selects is and the benefits of joining this program.

[Unique Identifier Header FAQs](#)

Learn what a Unique Identifier Header is and how it is used.

APPENDIX ATTACHMENT 2

AOL Privacy Policy

Last updated: June 23, 2015

AOL is now part of the Verizon family of companies. Additional privacy practices are described in the [Verizon Privacy Policy](#). In the event of a conflict between this Privacy Policy and the Verizon Privacy Policy, the AOL Privacy Policy will control when you are on an AOL site or using an AOL product or service.

At AOL, it's our mission to provide users with rich, interactive online experiences. From Pulitzer-Prize winning journalism on the Huffington Post, to the latest technology news on TechCrunch, to up-to-the-minute traffic information on MapQuest, our websites, apps, and other services and software are designed to keep you informed, entertained and delighted. We also operate some of the industry's best-known advertising services, including Adap.tv and Advertising.com.

We're always working to make our services even better. One of the ways we do that is by analyzing information we collect and receive about users in order to figure out what they might be interested in. This helps us develop more engaging content and provide more effective advertising, which enables us to keep most of our services free.

This Privacy Policy describes how we handle the information we collect and receive about users. There are three things you should keep in mind as you read it:

- First, the Privacy Policy applies to AOL services that link to or refer to this Privacy Policy. These services include websites, mobile apps, other online services and anything else that links to or refers to this policy. To keep things simple, we refer to all these services as our "Services."
- Second, the Privacy Policy applies no matter what computer or device you use to access our Services.
- Third, we may provide additional information about the privacy practices of some of our Services. Although this Privacy Policy applies to all AOL services that refer or link to it, you should read the additional information, too. Some of this information is linked from various places in the Privacy Policy, and some is available through the individual Services that you use.

We've done our best to keep this Privacy Policy short and simple, but if you have any questions about it, we hope you'll [let us know](#).

Information We Collect and Receive

We collect and receive information about users in a few different ways:

- **Information you give us**. You can give us information directly. For example:
 - When you sign up for an [AOL account](#) you may give us information such as your name, zip code, and date of birth;
 - When you purchase one of our paid services, you give us your billing information, which may include your credit card data;

- When you use **Moviefone**, you can give us your zip code so that we can tell you where and when movies are playing;
- When you post comments in response to a story or video on any of our Services, we-and other users-receive that information; and
- When you use the "**My Portfolios**" feature on **DailyFinance**, you can give us information about your investments so that we can provide you with up-to-the-second market news and commentary relevant to your holdings. (Your use of AOL financial features is subject to additional **privacy terms**.)
- When you otherwise contact us or provide us information directly.
- **Information we collect or receive when you use our Services**. We also collect or receive information when you use our Services. We collect some of this information using **cookies, web beacons, and other technologies**. Depending on how you access and use our Services, we may receive:
 - *Log information*. This is information we automatically collect and store when you use our Services or other companies' websites and apps in the **AOL Advertising Network**. It may include, for example:
 - Information about your interactions with the websites, apps, and other services you use, the content you view, the search queries you submit, and information in **cookies and similar technologies**;
 - Information about how you access those websites, apps, and other services, your browser or operating system, your Internet Protocol ("IP") address, and the website you visited before visiting our Services.
 - *Device information*. This is information we automatically collect and store about the device you use when you access our Services or the services in the **AOL Advertising Network**. (Note that by "device," we mean anything you use to access our Services. For more information about our privacy practices in connection with mobile devices, please review the **Supplemental Mobile Terms of Service and Privacy Policy**.) Device information includes, for example:
 - The type of device you're using (e.g., an iPhone);
 - Certain **device identifiers** which may be unique to your device; and
 - Your Internet service provider.

- *Location information.* This information can include, for example, your device's GPS signal and information about nearby WiFi networks and cell towers. We get this information when you use location-enabled services like MapQuest, which can give you driving directions based on your current location.
- *Other information.* Please note that AOL may use information about your use of certain AOL communication tools (for example, AOL Mail and AOL Instant Messenger); however, when you use AOL communication tools, AOL does not read your private online communications without your consent.
- **Information from third-party sources.** We may receive additional information about you that is publicly or commercially available and combine that with the information we have collected or received about you in other ways. Also, we receive information about you when you choose to connect with social networking services while using our Services. Learn more about how that works [here](#).

Additionally, when you use AOL software (such as the AOL desktop software, AOL toolbars, or AIM), we may collect information about other software on your device for the limited purposes of providing the service you are using and improving the security of our services.

How We Use the Information We Collect and Receive

We use the information we collect and receive for the following general purposes:

- **To provide our Services.** We use the information we collect and receive to provide you with the Services you use or request. For example:
 - If you request local movie show times from [Moviefone](#), we might use your location information to provide you with times at nearby theaters;
 - If you sign up to receive the daily headlines from [Huffington Post](#), we'll use your email address to deliver them to you; and
 - If you ask us to remember your login information for AOL Services, we'll use information stored in cookies when you return to those websites.
- **To improve our Services.** We also use the information we collect and receive to provide content and advertising that people are likely to find relevant and engaging. For example:
 - If we notice that Huffington Post users in general prefer national political commentary, we might put that content in a special place on the website or in the app;
 - If we notice that a user is searching for sports cars on [AOL Autos](#), we might show the user an ad for a sports car on [AOL.com](#) or on other sites in the [AOL Advertising Network](#); and

- If we receive information from users that a Service isn't working properly, we may use that information to address any problem.
- **To provide effective advertising.** Many of our Services are supported by advertising, and some of our Services provide advertising on our websites and apps, and on third-party websites and apps. We use the information we collect and receive to make the advertising we provide more effective. Some of the ways we do this are:
 - Showing you ads based on your online activities, such as the websites and applications you use, the content you view, and the searches you submit on those applications
 - Limiting the number of times you see the same ad; and
 - Measuring the effectiveness of the ads we serve.

[Learn more](#) about advertising and privacy on our Services.

How We Share the Information We Collect and Receive

We don't rent or sell **personal information** to third parties for their marketing purposes. But we may share certain information we collect or receive with third parties to provide products and services you have requested, when we have your consent, or as described in this Privacy Policy.

We may share information with:

- **Affiliates.** The information one AOL **affiliate** receives can be shared among other AOL affiliates, including the Verizon family of companies.
- **Business partners.** We may share **non-personally identifiable information** with select business partners, who may use the information for a variety of purposes, including to provide you with relevant advertising.
- **Other parties in response to legal process or when necessary to protect our Services.** We may disclose your information-including the contents of your communications with other parties-to other parties, such as when we have a good faith belief that:
 - It is necessary to respond to lawful governmental requests or legal process (for example, a court order, search warrant, or subpoena);
 - The information is relevant to a crime that has been or is being committed;
 - An emergency exists that poses a threat to your safety or the safety of another person; or
 - It is necessary to protect the rights or property of AOL.
- **Other parties in connection with certain business transactions.** In the event that the ownership of AOL Inc. or an **affiliate** or their assets changes as a result of a merger, acquisition, sale of assets, or in the unlikely event of a bankruptcy, your information may be

transferred to another company. If we believe a transfer results in a material change in the use of the information we've collected or received about you, you will be given the opportunity to opt out of the transfer.

Companies that Provide Services to AOL

Companies that provide services to us or act on our behalf may have access to information about you. These companies are limited in their ability to use information they receive in the course of providing services to us.

Third Parties that Provide Content, Advertising Services, or Functionality on Our Services

Some of the content, advertising, and functionality on our Services may be provided by third parties that are not affiliated with us. Such third parties include:

- Advertising providers, which help us and our advertising customers provide ads that are tailored to users' interests and understand how users respond to those ads;
- Audience-measurement companies, which help us measure the overall usage of our Services and compare that usage to other online services; and
- Social networking services (like Facebook, Twitter, LinkedIn, and Google) that enable you to login to certain of our Services and to share things you find on our Services with your social network.

These and other third parties may collect or receive information about your use of our Services, including through the use of [cookies](#), [web beacons](#) and [other technologies](#), and this information may be collected over time and combined with information collected on different websites and online services.

Note that some of these companies participate in industry-developed programs designed to provide consumers with choices about whether to receive targeted ads. To learn more, please visit the websites of the [Network Advertising Initiative](#) and the [Digital Advertising Alliance](#). For more information about privacy and advertising on our Services, please visit [Advertising, Analytics and Privacy](#).

If you choose to connect with a social networking service, such as Facebook, we may share information with that service, and that service may share information about you with us. We may use the information for the reasons explained in this Privacy Policy, but the main reason we use it is to make your experience on our Services more personal and social. For example, we might show you what content is popular among your connections on the social networking service or give you a glimpse of what your friends are saying about that content.

It's important to remember that we don't control the privacy practices of these (or any other) third-party services. So we encourage you to read the privacy policies of the services before connecting to them.

"Do Not Track" Signals

Some web browsers may transmit "do not track" signals to the websites and other online services with which the browser communicates. There is no standard that governs what, if anything, websites

should do when they receive these signals. AOL currently does not take action in response to these signals. If and when a standard for responding is established, we may revisit its policy on responding to these signals.

Choices

You have a number of choices about how we handle your information:

- If you're a registered AOL user, you can access your registration information and any billing or shipping information and edit this information by visiting "[My Account](#)."
- If you're a registered AOL user, you can visit [AOL Marketing Preferences](#) to review your marketing preferences and make choices about how your information may be used to provide marketing offers to you. Note that these preferences do not apply to communications that are directly related to your registration with AOL or the fulfillment of a specific transaction you have requested (for example, a service advisory from AOL or an acknowledgment of a purchase order).
- Visit our [Advertising, Analytics and Privacy](#) page to learn more about your choices related to use of your information for online advertising. You can also opt out of receiving targeted ads from AOL by visiting the [Digital Advertising Alliance's consumer choice page](#) and selecting AOL Advertising.
- Some of our Services ([AOL Search](#) and [Netscape ISP](#), for example) may also offer you the ability to manage and control information collected or used when you use these services.
- If you're using a mobile device, please visit our [Mobile Device Choices](#) page for information about the choices we provide to mobile users.

Our Commitment to Security

Although no one can guarantee the security of the information collected and received, we do employ a number of safeguards intended to mitigate the risk of unauthorized access or disclosure of this information. Examples of the types of safeguards we may provide (depending on the circumstances) include:

- Storing the data you provide in controlled facilities;
- Using HTTPS encryption when you authenticate (i.e., log into one of our Services), which helps prevent unauthorized access to your login credentials;
- Limiting access to personal information to employees who need that access to perform their jobs; and
- Providing company-wide training on privacy and data security.

Children's Privacy

Our Services are intended for a general audience. We do not knowingly collect, use, or disclose personal information from children under the age of 13 without prior parental consent, except as permitted by the Children's Online Privacy Protection Act. If you are a parent who consents to the collection of personal information from your child, you agree that your child may use all of our Services and that we may collect, use, and disclose your child's personal information consistent with AOL's [Important Note to Parents](#) and this Privacy Policy.

If you have questions concerning our information practices with respect to children, or if you would like to review, have deleted, or stop the further collection of your child's personal information, you may contact us:

By mail:

AOL Children's Online Privacy

ATT: H2A:C05

22000 AOL Way

Dulles, VA 20166-9302

By phone: (888) 206-6088

[By email](#)

International users

AOL is based in the United States, and, regardless of where you use our Services or otherwise provide information to us, the information may be transferred to and maintained on servers located in the U.S. Please note that any information we obtain about you will be stored in accordance with U.S. privacy laws, regulations, and standards, which may not be equivalent to the laws in your country of residence. By using our Services or by providing us with your information, you consent to this collection, transfer, storage, and processing of information to and in the U.S.

AOL Inc. complies with the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland. AOL has certified that it adheres to the [Safe Harbor Privacy Principles](#) of notice, choice, onward transfer,

security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view AOL's certification, please visit <http://www.export.gov/safeharbor/>.

How to Contact Us

If you have questions or concerns about this Privacy Policy or about AOL's privacy practices in general, please send us an [email](#).

Changes to This Privacy Policy and Additional Information

We may update this Privacy Policy from time to time, and so you should review this Policy periodically. If there are significant changes to AOL's information practices, you will be provided with appropriate online notice.

APPENDIX ATTACHMENT 3



Full Privacy Policy

Protecting our customers' privacy is an important priority at Verizon and we are committed to maintaining strong and meaningful privacy protections. The privacy of your information is a significant responsibility and we value the trust you place in us.

Our Privacy Policy is designed to inform you about the information we collect, how we use it, and your options regarding certain uses of this information. This policy also describes privacy rights you have under certain federal laws.

This policy applies to website visitors and Verizon customers in the United States. It applies across the [Verizon family of companies](#) and the products and services they provide. The Verizon family of companies includes the companies and joint ventures controlled by Verizon, including the Verizon telephone companies, Verizon Enterprise Solutions, Verizon Wireless, AOL and Verizon Online.

Additional privacy practices that apply to Fios, Verizon Wireless, AOL and hum services are also described in this policy. Supplemental privacy policies for AOL companies and the services they provide are described in the [AOL privacy policy](#). In the event of a conflict between the Verizon privacy policy and the AOL privacy policy, the AOL policy will control when you are on an AOL site or using an AOL product or service.

View [policies for Verizon Enterprise Solutions customers](#) outside the United States. Also, certain services offered to consumers as well as contracts between Verizon and its business customers (both U.S. and international) may contain additional privacy-related terms and conditions that are presented to you in other ways.

[See recent changes to the privacy policy](#)

Information we collect and how it is used

We collect information when you communicate with us and when you use our products, services and sites. This includes information you provide such as name and contact information, images, voice recordings or prints, the reason for contacting us, driver's license number, Social Security Number and payment information. Service usage information we collect includes call records, websites visited, wireless location, application and feature usage, network traffic data, product and device-specific information and identifiers, service options you choose, mobile and device numbers, video streaming and video packages and usage, movie rental and purchase data, TV and other video viewership, and other similar information.

We use this information to establish, monitor and maintain your account and billing records; measure credit and payment risk; provide account-related services; deliver and maintain your products and services; help you with service-related issues or questions; manage and protect our networks, services and users from fraudulent, abusive, or unlawful uses; help us improve our services and research and develop new products and services; authenticate you; determine your eligibility for new products and services and contact you with marketing offers.

When you contact us or we contact you, we may monitor or record that communication or keep a record of the transaction to help us train employees and better serve you.

We may automatically measure and monitor network performance and the performance of your connections to improve your, or our, service levels and products. If you contact us for service support, we also may access information about your computer, wireless device or other device settings to provide customized technical support or to install specific applications or services that you use or that are necessary to the applications or services you use.

Information about your use of Verizon products and services may be aggregated or otherwise de-identified for business and marketing uses by us or by third parties. For example, aggregate or de-identified data may be used to improve our services, measure and analyze the use of services and to help make services and advertising more relevant to you. You can opt out of certain of these uses, for example the [Verizon Relevant Mobile Advertising](#) and [Business and Marketing Insights](#) programs discussed below.

When you establish an online account or register on our sites or apps, we may collect information about your user identification, password and secret questions and answers. We use this information to authenticate you when you sign in.

Verizon will obtain your affirmative consent before we use information we gathered in the course of providing broadband Internet access services about your visits over time to different non-Verizon websites to customize ads specifically to you. One such program is [Verizon Selects](#).

Please note that Verizon is not responsible for information, content, app or services provided by others. Before you access, use, link to or download a service or app on your computer, television, wireless or other device, you should review the associated terms of service and privacy policy. Personal information you submit in those contexts may be read, collected or used by the service or app provider and others in ways that are different from described here.

Information provided to us by third parties

When you purchase products or apply for service with us, we may obtain credit information about you from outside credit reporting agencies to help us with customer authentication and credit-related decisions. If you lease your residence, we may have information about how to reach your landlord and whether landlord permission is required to install our facilities.

Verizon obtains information from outside companies such as those that collect consumer information including demographic and interest data. Examples of this information include gender, age range, education, sports enthusiast, frequent diner or pet owner. We use this data and combine it with other information we have about you to help us predict your preferences, to direct marketing offers that might be more relevant to you, and to help us better analyze customer information for various purposes including credit and payment risk.


When you use social media credentials to login to or otherwise interact with a Verizon site or offer, we may collect information about your social media profile, such as your interests, "likes" and friends list. We may use this information, for example, to personalize your Verizon experiences and marketing communications, to enhance our services and to better serve you. You can control this data sharing via options in your social media accounts.

We also obtain contact information and other marketing lead information from third parties, website "refer-a-friend" options or social media platforms and may combine it with information we have to contact you or direct Verizon's marketing offers to you.

Information collected on Verizon websites and apps

When you use Verizon websites and apps, information is collected about your device and your visit including browsing, searching and buying activity as you interact with our sites and apps; IP address; mobile telephone, device numbers and identifiers; account information; web addresses of the sites you come from and go to next; and information about your connection, including your device's browser, operating system, platform type and Internet connection speed. We use this information for

operational, performance measurement and other business purposes; and to help us deliver more relevant Verizon marketing messages on our websites, on non-Verizon websites, by our representatives, via email, or via other Verizon services or devices. This information is also used to tailor the content you see, manage the frequency with which you see an advertisement, tailor advertisements to better match your interests and understand the effectiveness of our advertising. We also may use this information to assess the effectiveness of our sites and to help you should you request help with navigation problems on these sites. Additional information about the information collected on AOL websites is described in the [AOL privacy policy](#).

Certain Verizon vendors may place and read [cookies](#) on our sites to help us deliver Verizon marketing messages on our sites and on non-Verizon sites. We require that these vendors provide consumers with the ability to opt out of their use of information for these purposes. In accordance with [industry self-regulatory principles](#), you should see this icon in  or around Verizon advertisements that are delivered on other sites using information collected on our sites. Clicking on this icon will provide information about the companies and data practices that were used to deliver the ad and will also describe how you may opt out of this type of advertising program. Additional information on the choices available to you for the use of your information for advertising purposes can be found in the "[How to limit the sharing and use of your information](#)" section below. [View information about "cookies" and related technologies](#)

Information you provide

When you contact us for information about products and services or when you enter a Verizon-sponsored or affiliated contest, sweepstakes or promotion, we may use the information you supply to provide you with information about Verizon services, programs and offerings. Certain promotions may require that we disclose information such as contest winners or provide information for prize fulfillment, and as required by law or permitted by the promotion's official rules. Information you provide on our websites about your preferred location and other preferences may be used to provide you with more relevant product recommendations, services and special offers.

If you provide information to us in the context of an event or promotion that Verizon sponsors with another organization, or if you visit a co-sponsored site or use a co-sponsored service, you also may be providing information to the co-sponsor. You should refer to that co-sponsor's privacy policy for information about its practices which may differ from Verizon's practices.

We also collect information from you when you participate in surveys or provide other feedback to us regarding our products or services, when you register to receive news or public policy updates, or when you apply for a job with or a grant from Verizon. We use this information only for the purpose for which you provide it.

Verizon may send you emails that communicate information about your account or about products, services, marketing offers or promotions that may be of interest to you. When you open a Verizon email or click on links within these emails, we may collect and retain information to provide you with future communications that may be more interesting to you. Please note that Verizon will not ask you to send us, via email, sensitive personal or account information.

Additional information for Verizon Wireless customers

Verizon Wireless includes a [unique identifier](#) in certain web traffic from your mobile device. The identifier is used to help deliver relevant advertising and to deliver other services such as authenticating devices on the network. If you opt out of the [Relevant Mobile Advertising](#) program and you have not joined Verizon [Selects](#), or if you activate certain types of lines that are not eligible to participate in our advertising programs, Verizon Wireless will stop inserting the [Unique Identifier Header \(UIDH\)](#). The identifier will continue to appear for a short period of time while we are updating our systems.

Verizon Wireless collects and uses mobile device location data for a variety of purposes, including to provide our mobile voice and data services, emergency services, and our and third-party location-based apps and services such as navigation, weather, mapping and child safety apps or tools. Verizon apps that use location information provide choices about the use of this information.

Many types of wireless apps and services use mobile device location data, including apps provided by other companies and wireless device operating systems. When you are considering new apps or services, you should carefully review the location-based services' or app providers' privacy policies to learn how they collect and use your information.

Verizon-supplied system application software may be present on your wireless device to enable automatic installation of apps when you activate your device and with your consent at later times. For example, at your request, this software may be used to install or open an app or your browser to a specific page based on an interaction you are having with a company's telephone voice response system. The software collects certain usage information about the actions it takes, including first open and uninstalls. You can delete or disable apps installed by this software at any time.

Verizon Wireless does not publish directories of our customers' wireless phone numbers, and we do not provide or make them available to third parties for listing in directories unless you request that we do so.

Information about the Cable Act

To the extent that Section 631 of the Communications Act of 1934, as amended (the "Cable Act") applies to services you purchase, it entitles you to know about the personally identifiable information a cable service provider collects. This includes the nature of the use and disclosure of this information and to whom it may be disclosed, how long personally identifiable information is maintained, and how subscribers may access it. In addition, the Cable Act imposes limits on the collection and disclosure of personal information and gives subscribers the ability to enforce their privacy rights. (Personally identifiable information does not include aggregate data that does not identify a particular person).

The Cable Act allows a provider to use its cable system to collect personally identifiable information necessary to render a cable service or other services provided to subscribers and to detect and prevent unauthorized access to services. Additional personally identifiable information may be collected with the subscriber's prior consent. Personally identifiable information may be used or disclosed without the subscriber's consent where necessary to render services, and to conduct legitimate business activities related to services provided.

We may be required by law to disclose personally identifiable information to a governmental entity to comply with valid legal process, such as warrants, court orders or subpoenas, but we will not disclose records revealing your selection of video programming unless we receive a court order indicating that the governmental entity has made a specified showing of relevance and you were afforded an opportunity to contest the order. We may be required to disclose personally identifiable information (including your selection of video programming) to a non-governmental entity to comply with a court order, after you have been provided notice.

If you believe that your privacy rights have been violated, please [e-mail us](#) and we will work with you to address your concerns. If you believe that you have been aggrieved as a result of a violation of the Cable Act, you may enforce the limitations imposed by the Cable Act through a civil action in a United States district court seeking damages, attorney's fees, and litigation costs. Other rights and remedies may also be available to you under federal or other applicable laws.

The Cable Act permits the disclosure of customer names and addresses as long as a subscriber has been provided with the opportunity to prohibit or limit this disclosure and the disclosure does not reveal, directly or indirectly, the subscriber's viewing or other uses of the cable or other services

provided. If we intend to share data in this way, we will provide you with the opportunity to prohibit or limit this type of sharing.

Additional Information for hum service

hum service includes vehicle diagnostics, vehicle location assistance, one-button emergency calling, automated alerts to emergency personnel when a potential accident is detected, and roadside assistance services as well as possible discounts on travel, automotive, car rental and other offers. When installed in your car, the hum system collects information about your vehicle's performance and maintenance characteristics, as well as vehicle location and use information (including trip distances, acceleration, deceleration, turning, speed and revolutions per minute). In addition to other uses described in this policy, this information will be used to develop and provide a driving tips feature planned for introduction in 2016. This feature is expected to rate your overall driving and suggest ways in which driving could potentially be improved.

Information that identifies your vehicle and other personal information may be shared as described in the information sharing sections of this policy as well as when it is necessary to provide various hum service features, such as alerting emergency personnel of your location if a crash is detected, helping authorities locate your vehicle if you report it stolen or helping roadside assistance locate your vehicle.

hum information may also be used on its own or in combination with other Verizon information to determine aggregate insights about hum users. For example, a company may find it valuable to know the number of vehicles on different roads at various times during the day and the percent of drivers of those vehicles that are in a certain age range. hum information may also be shared with third parties in a way that does not identify you personally. For example, it may be used to provide traffic reporting and similar services or to inform car manufacturers about characteristics of different vehicle models.

Advertising and insight programs

<p>Relevant Mobile Advertising Program</p>	<p>The Verizon Wireless Relevant Mobile Advertising program, part of the AOL Advertising Network, helps make marketing you see more personalized and useful to you across the devices and services you use.</p> <p>The Relevant Mobile Advertising program uses your postal and email addresses; certain information about your Verizon Wireless products and services such as your device type; and demographic and interest categories we get from other companies such as your gender, age range and interests (i.e. sports fan, frequent diner or pet owner). This information may be combined with information the AOL Advertising Network collects when you use AOL services and visit third-party websites where AOL provides advertising services (such as web browsing, app usage and location), as well as information that AOL obtains from third-party partners and advertisers. The advertising program uses online and device identifiers including AOL browser cookies, advertising IDs from Apple and Google, and one created by Verizon, known as a Unique Identifier Header or UIDH.</p> <p>We do not share information that identifies you personally as part of these programs other than with vendors and partners who do work for us. We require that these vendors and partners protect the information and use it only for the services they are providing us. You have a choice about participating in this program.</p>
<p>Business and</p>	<p>Verizon Wireless uses certain customer information to create aggregate</p>

<p>Marketing Insights</p>	<p>business and marketing insights. The program uses Information about how you use your mobile device, including web browsing, apps and features you use and the location of your device, as well as certain information about your Verizon products and services (such as device type and amount of use) and information we obtain from other companies (such as gender, age range and interests). We may combine this information in a manner that does not personally identify you and use it to prepare aggregated business and marketing insight that we may use ourselves or share with others for their use. We may also share location information with others in a way that does not personally identify you so that they may produce aggregate business and marketing reports. You have a choice about whether your information is included in these reports.</p>
<p>Relevant Online Advertising</p>	<p>The Relevant Online Advertising program helps advertisers better reach our wireline Internet access customers using the postal address we have for you; certain information about your Verizon products and services – such as broadband and video service features; and demographic and interest information provided to us by other companies – such as gender, age-range, sports fan, frequent diner or pet owner. This information is used to predict whether you fit within an audience an advertiser is trying to reach. We do not share information that identifies you personally as part of these programs other than with vendors and partners who do work for us. We require that these vendors and partners protect the information and use it only for the services they are providing us. You have a choice about participating in this program.</p>
<p>Relevant TV Advertising</p>	<p>Verizon’s Relevant TV Advertising program helps advertisers reach Fios television customers with advertisements that may be more relevant to their interests. We do not share information that identifies you personally as part of these programs other than with vendors and partners who do work for us. We require that these vendors and partners protect the information and use it only for the services they are providing us. The ads may appear on a variety of platforms where Fios television customers can access video content. We help advertisers deliver ads to audiences based on demographic and interest information (such as gender, family size, and luxury car owner) we obtain from other companies, your address and certain information about your Verizon products and services (such as service packages purchased, video on-demand purchases and program viewing data). You have a choice about receiving this type of advertising and you can opt out online.</p>

Additional information for AOL services

AOL products and services include online services such as AOL.com, The Huffington Post, TechCrunch and MapQuest; AOL Mail and AIM; and advertising services, including ONE by AOL and Advertising.com. Many of AOL's free services are supported by the ads displayed on those services. AOL also provides a variety of online advertising services to other companies that place ads on our services and elsewhere.

The [AOL Privacy Policy](#) provides additional information about the collection and use of information from any devices you use to access or connect to AOL branded websites, services and software as well as many websites owned by or affiliated with AOL and operating under different names. It also describes the collection and use of information by AOL Advertising and your related choices. In the event of a conflict between this Privacy Policy and the AOL Privacy Policy, the AOL Privacy Policy will control when you are on an AOL site or using an AOL product or service.

Information we share

Information shared within the Verizon family of companies:

Verizon shares customer information within our family of companies for a variety of purposes, including, for example, providing you with the latest information about our products and services and offering you our latest promotions. You can limit the sharing of certain types of customer information, known as Customer Proprietary Network Information, or CPNI, within the Verizon family of companies for marketing services to you other than your current services.

Customer Proprietary Network Information (CPNI) is information that relates to the type, quantity, destination, technical configuration, location, amount of use and related billing information of your telecommunications or interconnected Voice over Internet Protocol (VoIP) services. Federal law governs our use and sharing of CPNI.

Information shared outside the Verizon family of companies:

Except as explained in this Privacy Policy, in privacy policies for specific services, or in agreements with our customers, Verizon does not sell, license or share information that individually identifies our customers, people using our networks, or website visitors with others outside the Verizon family of companies that are not performing work on Verizon's behalf without the consent of the person whose information will be shared.

Verizon uses vendors and partners for a variety of business purposes such as to help us offer, provide, repair, restore and bill for services we provide. We share information with those vendors and partners when it is necessary for them to perform work on our behalf. For example, we may provide your credit card information and billing address to our payment processing company solely for the purpose of processing payment for a transaction you have requested. We require that these vendors and partners protect the customer information we provide to them and limit their use of Verizon customer data to the purposes for which it was provided. We do not permit these types of vendors and partners to use this information for their own marketing purposes.

As described in more detail in other sections of this policy, Verizon also may share certain information with outside companies-, for example, to assist with the delivery of [advertising campaigns](#), or preparing and sharing aggregate reports. This information does not identify Verizon customers individually.

Verizon provides the names, addresses and telephone numbers of wireline telephone customers to directory publishers and directory assistance services unless a non-published or non-listed phone number has been requested.

We may disclose information that individually identifies our customers or identifies customer devices in certain circumstances, such as:

- to comply with valid legal process including subpoenas, court orders or search warrants, and as otherwise authorized by law; in cases involving danger of death or serious physical injury to any person or other emergencies;
- to protect our rights or property, or the safety of our customers or employees;
- to protect against fraudulent, malicious, abusive, unauthorized or unlawful use of or subscription to our products and services and to protect our network, services, devices and users from such use;
- to advance or defend against complaints or legal claims in court, administrative proceedings and elsewhere;
- to credit bureaus or collection agencies to determine credit risk, for reporting purposes or to obtain payment for Verizon-billed products and services;
- to a third-party that you have authorized to verify your account information;
- to outside auditors and regulators; or

- with your consent.

When you purchase services offered jointly by Verizon and one of our partners, customer information may be received by both Verizon and our partner that is providing your service. For these jointly offered services, you should also review the partner company's privacy policy which may include practices that are different from the practices described here.


If Verizon enters into a merger, acquisition or sale of all or a portion of its assets or business, customer information will also be transferred as part of or in connection with the transaction.

Information provided to or used by advertising entities or social networks

You may see third-party advertisements on some Verizon websites, services, apps and devices. Some advertisements are chosen by companies that operate on our sites and other sites (for example, ad servers, ad networks, or technology platforms) to place ads on behalf of advertisers. These companies may place and access cookies on your device to collect information about your visit on websites and may collect device advertising identifiers from your mobile operating system to learn about your use of apps, including ours. The information they collect from our sites and apps is in a form that does not identify you personally and may be combined with similar data they obtain from other websites and apps to help advertisers better reach audiences they wish to target. Targeting may be accomplished by tailoring advertising to interests that they infer from your interactions on our sites and apps and your interaction with other sites and services where these companies also are present. AOL also provides these types of services to advertisers; more information is described in the [AOL privacy policy](#).

If you choose to interact with specific advertisers who advertise on our apps sites or services, the information you provide to them is subject to the conditions of their specific privacy policies.

Advertising that is customized based on predictions generated from your visits over time and across different websites is sometimes called "online behavioral" or "interest-based" advertising. In accordance with [industry self-regulatory principles](#), we require that companies disclose when they are using online behavioral advertising programs to deliver third-party ads on our sites or collecting information about your visit to our sites for these purposes and give consumers the ability to opt out

of this use of their information. You will see an icon  in or around third-party advertisements that are delivered on our sites using behavioral advertising programs. Clicking on this icon will provide additional information about the companies and data practices that were used to deliver the ad as well as information on how you may opt out of these advertising programs. Additional information about your options regarding the use of your information for advertising purposes can be found below. [View additional information about online behavioral advertising](#). Please note that Verizon does not have control over or access to information contained in the cookies that are set on your computer by ad servers, ad networks or third-party advertisers.

Similarly, advertising may be customized based on predictions developed from your use of applications and industry self-regulatory principles also apply. This type of advertising involves the use of device advertising identifiers. [View information about opting out of this use of your device advertising identifier](#).

[View information about "cookies" and related technologies](#)

We also may permit advertisers on our sites, apps and services to place ads based on certain information we have about your Verizon products and services as well as geographic and demographic data. Information used for this purpose does not identify you individually.

Verizon websites and services may include social network or other third-party plug-ins and widgets that may provide information to their associated social networks or third-parties about your

interactions with Verizon pages you visit or services you use, even if you do not click on or otherwise interact with the plug-in or widget. [View information about "cookies" and related technologies](#)

How to limit the sharing and use of your information.

You have choices about how Verizon shares and uses information.

Customer Proprietary Network Information (CPNI)

Customers of Verizon telecommunications and VoIP services may choose to limit the use and sharing of CPNI for Verizon's marketing services outside of services you currently have. Notice about our use and sharing of CPNI and the choices you have may be provided on your monthly bill, over the phone, via text, in contracts or in other ways.

Verizon Wireline consumers and certain business customers may opt out by calling 1-866-483-9700. Verizon Wireless consumer and certain business customers may call 1-800-333-9956. Other customers may decline to provide or withdraw CPNI consent by following the instructions in the Verizon notice seeking consent.

[View CPNI notices for Verizon Wireline and Verizon Wireless](#)

Telemarketing

Federal "Do Not Call" laws allow you to place your phone numbers on the National Do Not Call Registry to prevent telemarketing calls to those numbers. To add your numbers to this list, please call 1-888-382-1222 or visit the [National Do Not Call Registry](#).

Most telemarketing laws allow companies to contact their own customers without consulting the federal or state Do Not Call list. If you would like to be removed from Verizon's residential telemarketing list, please contact us at 1-800-VERIZON. If you would like to be removed from the Verizon Wireless telemarketing list, please contact us at 1-800-922-0204. Please allow 30 days for your telephone number to be removed from any sales programs that are currently underway.


Marketing e-mail, text messages, postal mail and door-to-door calls

Marketing emails you receive from Verizon, include an unsubscribe instruction (usually found at the bottom of the email) that you may use to opt out of receiving future marketing-related emails.

You may opt out of receiving marketing-related postal mailings or prevent door-to-door marketing solicitations from Verizon by calling 1-800-VERIZON. You may opt out of receiving marketing-related postal mailing or prevent text message marketing by Verizon Wireless by calling 1-800-922-0204. You may opt out of receiving marketing-related postal mailing or prevent text message marketing by Verizon Vehicle service by calling 1-800-711-5800. Text message solicitations from Verizon also contain an "unsubscribe" feature that you can use to prevent future marketing text messages from us. Please note that Verizon may use bulk mail service for some marketing mailings. These services deliver offers to all homes in a neighborhood or zip code. This type of mailing will continue even if you opt out of receiving marketing-related postal mailings from Verizon.

Information used for online advertising

You have choices about whether certain information collected on websites, including Verizon's, is used to customize advertising based on predictions generated from your visits over time and across

different websites and apps. When you see this icon  in or around an advertisement you can click on the icon to see additional information on the companies and data practices that were used to deliver the ad and descriptions of how you may opt out of these advertising programs. You may also visit [Digital Advertising Alliance's Consumer Choices](#) to learn more or to limit the collection of

information by these parties. Similarly, many mobile devices offer controls you can set to limit the advertising use of information collected across mobile apps on your device. AOL also provides these types of services to advertisers; more information is described in the [AOL privacy policy](#).

Please note that many opt outs use browser cookies or device controls and are specific to the device and browser you are using. If you buy a new computer, change web browsers or devices or delete the cookies on your computer, you may need to opt out again. In addition, ads you receive may still be tailored using other techniques such as publisher, device or browser-enabled targeting. You should check the privacy policies of the products, sites, apps and services you use to learn more about any such techniques and your options.

You also can limit the collection of certain website information by deleting or disabling cookies. Most computers' Internet browsers enable you to erase cookies from your computer hard drive, block all cookies, or receive a warning before a cookie is stored. Disabling cookies may prevent you from using specific features on our sites and other websites, such as ordering products or services and maintaining an online account. Cookies must be enabled for you to use your Verizon e-mail account. [View information about "cookies" and related technologies](#)

Advertising programs:

- Verizon Wireless customers may opt out of the Relevant Mobile Advertising program by following the instructions here or by calling us at 1-866-211-0874.
- Verizon broadband Internet access customers may opt out of the Relevant Online Advertising program described above by [following these instructions](#).
- Customers may opt out of Verizon's Relevant TV Advertising program by [following these instructions](#).

If you opt out online, you will need your account user ID and password. Also, please note that you will receive ads whether you participate in these programs or not, but under these programs, ads may be more personalized and useful to you.

Business and Marketing Insights

Verizon Wireless customers may choose not to have their information included in the creation of aggregated business and marketing insights that do not specifically identify any individual customers. You may opt out by calling 1-866-211-0874 or by visiting [your privacy choices page in My Verizon](#). Please note that if you have multi-line account, you should indicate your opt out choice for each line. If you add a line or change a telephone number, you will need to update your privacy choices.

AOL choices

You have choices about how AOL uses information. To learn more visit the [AOL Privacy Policy](#).

Working together to keep children safe.

Verizon recognizes that online service providers must be vigilant in protecting the safety and privacy of children online. We do not knowingly market to or solicit information from children under the age of 13 without obtaining verifiable parental consent.

To learn more about AOL's information practices with respect to children under 13, please review [AOL's Important Note to Parents](#).

Regrettably, there are those who use the Internet to view, store and distribute child pornography (or who engage in other types of illegal activity involving children). Child pornography is subject to severe criminal penalties and using the Verizon network to view, store or distribute it violates our

service contracts. The Verizon network may not be used by customers in any manner for the storage, transmission or dissemination of images containing child pornography and we will report any instances of such activity of which we become aware to the appropriate law enforcement authorities.

If you have a complaint about child pornography, the soliciting of children for sexual activity, or any other illegal or inappropriate activity involving children on a Verizon service, report it to us by [sending an e-mail](#). Please include the words "child porn" in the subject line of your email. You can also make a report directly to the National Center for Missing and Exploited Children through [CyberTipline](#).

Additional Internet safety resources and information are available at:

- <http://www.netsmartz.org/>
- <http://www.wiredsafety.org/>
- <http://www.onguardonline.gov/>
- <http://www.common sense media.org/>
- <http://www.stopbullying.gov/>
- <http://www.cyberbullying.us/>
- <http://www.connectsafely.org/>
- <http://www.accreditedschoolsonline.org/bullying-awareness-guidebook/>

[Learn more about online safety tips and resources](#)

Information security and data retention

Verizon has technical, administrative and physical safeguards in place to help protect against unauthorized access to, use or disclosure of customer information we collect or store, including social security numbers. Employees are trained on the importance of protecting privacy and on the proper access to, use and disclosure of customer information. Under our practices and policies, access to sensitive personally identifiable information is authorized only for those who have a business need for such access. Personally identifiable and other sensitive records are retained only as long as reasonably necessary for business, accounting, tax or legal purposes.

Although we work hard to protect personal information that we collect and store, no program is 100% secure and we cannot guarantee that our safeguards will prevent every unauthorized attempt to access, use or disclose personal information. Verizon maintains security and incident response plans to handle incidents involving unauthorized access to private information we collect or store.

If you become aware of a security issue, please contact [Verizon's Security Control Center](#). We will work with you to address any problems.

Verizon often publishes helpful information about a wide range of scams that you may encounter. [Learn more about Internet and phone scams and tips on how to protect yourself](#)

Accessing and updating your information

We strive to keep our customer records as accurate as possible. You may correct or update your Verizon customer information by calling a Verizon customer service representative at 1-800-VERIZON or by accessing your account online and providing the updated information there. Similarly, updates can be made to your Verizon Wireless account by calling a Verizon Wireless customer service representative at 1-800-922-0204 or [contact us online](#). Verizon Enterprise Services customers may update their information by contacting their account manager. Verizon Vehicle customers may change or update their contact information by calling 1-800-711-5800. Registered

AOL users may access and update their registration information and any billing or shipping information by visiting [My Account](#).

Fios and other customers served over our fiber-to-the-premises network who would like to see their personally identifiable information, may [e-mail us](#) to arrange a time and convenient location to do so during business hours. You will need to provide proper identification and you may examine records that contain personally identifiable information about you and no one else. If you believe any of your personally identifiable information is inaccurate, we will work with you to ensure that corrections are made. Verizon reserves the right to charge you for the cost of photocopying any documents you request.

Links to and from non-Verizon websites and content

Verizon websites, apps and platforms may contain links to non-Verizon sites and Verizon apps or other content may be included on web pages and web sites that are not associated with Verizon and over which we have no control. We are not responsible for the content on these sites or platforms or the privacy policies and practices employed by these sites and platforms. We recommend that you review the policies and practices of the sites you visit.

Information sharing: Blogs and social networking

Some Verizon websites, apps and services may allow you to participate in web log ("blog") discussions, message boards, chat rooms, and other forms of social networking and to post reviews. Please be aware that these forums are accessible to others. We urge you to not submit any personally identifiable information to these forums because any information you post can be read, collected, shared, or otherwise used by anyone who accesses the forum. Verizon is not responsible for the information you choose to submit in these forums. If you post content to information sharing forums, including any information about the movies you rent or view, you are doing so by choice and you are providing consent to the disclosure of this information.

Changes to this policy

We reserve the right to make changes to this privacy policy, so please check back periodically for changes. You will be able to see that changes have been made by checking to see the effective date posted at the end of the policy. If Verizon elects to use or disclose information that identifies you as an individual in a manner that is materially different from that stated in our policy at the time we collected that information from you, we will give you a choice regarding such use or disclosure by appropriate means, which may include use of an opt out mechanism.

[View recent changes to privacy policy](#)

Updated May 2016

© 2009, 2011-2016 Verizon. All Rights Reserved.

Contact us

If you have questions, concerns or suggestions related to our Privacy Policy or our privacy practices, [e-mail us](#) or contact us at:

Verizon Privacy Office
1300 I Street, NW
Suite 400 West
Washington, DC 20005
Fax: 202-789-1432

APPENDIX ATTACHMENT 4

Relevant Mobile Advertising FAQs

General Information

1. What is Relevant Mobile Advertising?

The Relevant Mobile Advertising program, part of the [AOL Advertising Network](#), helps make marketing you see more personalized and useful to you across the devices and services you use.

Information used by the Relevant Mobile Advertising program includes your postal and email addresses; certain information about your Verizon Wireless products and services such as your device type; and demographic and interest categories we get from other companies such as your gender, age range, and interests (i.e. sports fan, frequent diner, or pet owner). This information may be combined with information the AOL Advertising Network collects when you use AOL services and visit third-party websites where AOL provides advertising services (such as web browsing, app usage, and location), as well as information that AOL obtains from third-party partners and advertisers. This information is described in the [AOL privacy policy](#).

The advertising program uses online and device identifiers including AOL browser cookies, advertising IDs from Apple and Google, and one created by Verizon, known as a Unique Identifier Header or UIDH. Unless you opt out of the Relevant Mobile Advertising program (and have not opted in to the separate [Verizon Selects](#) program), a UIDH is included in the address information of Internet requests going to Verizon companies (including AOL) and to a small number of partners to help deliver services unrelated to advertising. In addition, with your opt-in consent, for example when you opt in to the Verizon Selects program, the UIDH may be shared with partners who provide advertising services. Partners that receive the UIDH are authorized to use the UIDH only as part of the Verizon and AOL services and not for their own separate uses. More information about the UIDH can be found [here](#).

2. Is any of my personal information shared outside the Verizon family of companies?

We do not share information that identifies you personally as part of these programs other than with vendors and partners who do work for us. We require that these vendors and partners protect the information and use it only for the services they are providing us.

3. What types of devices will receive advertising?

Devices you have on your Verizon Wireless account and those you use to log in to My Verizon will receive ads. In addition, you may receive advertising on devices you use to connect directly to AOL sites and services, or on third party sites where AOL provides advertising services. If you share your mobile hotspot with others, ads relevant to you may also appear on other connected devices.

4. What types of accounts may be part of Relevant Mobile Advertising?

Most Verizon Wireless consumer and small business accounts are eligible to be included. Corporate, government and prepaid accounts are not eligible.

5. Will my device location be used?

Information Verizon Wireless has about the location of your mobile device is not used in the combined program. AOL offers its own services that involve the collection of location information, and location information that AOL collects or uses, as well as any location information provided by advertisers themselves, may be used by AOL. For example, if you allow the MapQuest app to collect and use your location information, that information may be used by AOL to help make advertising you see more relevant. More information can be found in the [AOL privacy policy](#).

6. Will information about my mobile web browsing be used?

Information Verizon Wireless has about web activity from your mobile device is not used in the program. Mobile and online web browsing information AOL independently collects is used.

7. Where will I see advertising?

You'll see advertising in the same places you see it today, such as on websites you visit or in apps you use.

8. Do I have a choice about the use of my Verizon Wireless information for the program? Do I have a choice about the insertion of the UIDH?

Yes, you can notify us that you do not want us to use your Verizon Wireless customer information by visiting www.vzw.com/myprivacy or by calling (866) 211-0874. If you have an account with multiple lines, you must indicate your privacy choices with respect to each individual line. If you opt-out of Relevant Mobile Advertising and you have not joined Verizon Selects, Verizon will stop including a UIDH in traffic coming from your device. The UIDH will still appear for a short period of time after you opt-out of the Relevant Mobile Advertising program. If you are a member of Verizon Selects, the UIDH will still be present even if you opt-out of Relevant Mobile Advertising. More information about the UIDH is available [here](#).

9. Do I have choices about the use of AOL information for the program?

You have [choices](#) about how AOL uses your information for advertising purposes. You can opt-out of receiving interest-based ads when you browse the web by visiting the [Digital Advertising Alliance's consumer choice](#) page and selecting "AOL Advertising." This opt-out choice will apply only to the browser you are using when you opt-out, so if you are using multiple browsers or devices, you will need to repeat this process on each. Please note that blocking or deleting cookies in your browser may cancel your choice to opt-out.

You can make your opt-out choice apply to any browser and device you use while signed into AOL by adjusting your [AOL Marketing Preferences](#).

You can also opt-out of receiving advertisements targeted to your mobile device by AOL by following the instructions provided at this [Mobile Device Choices](#) page.

10. Can I opt-out of these advertising programs using my browser controls?

No, using browser controls such as clearing cookies on your devices or clearing your browser history is **not** an effective way to opt-out of the Verizon and AOL advertising programs. Instead, if you want to opt-out, you should take the steps outlined above in #8 and #9.

11. Is the UIDH still present if I have opted-out of Relevant Mobile Advertising?

Verizon Wireless will stop including a [UIDH](#) after you opt-out of the Relevant Mobile Advertising program or activate a line that is ineligible. (Government and enterprise lines are examples of ineligible lines.) The UIDH will still appear for a short period of time after you opt-out or activate an

ineligible line. If you choose to participate in the Verizon Selects program, the UIDH will be present even if you have opted-out of the Relevant Mobile Advertising program.

12. If I decide to allow you to use my information for Relevant Mobile Advertising, can I change my mind later?

Yes, you can change your privacy choices at any time. When you opt-out, Verizon Wireless data will no longer be combined with AOL Advertising Network information and Verizon Wireless data will be removed by AOL from the information it uses to provide advertising to you. Please note that: (1) this is not applicable if you remain opted-in to the Verizon Selects program, and (2) information collected prior to the date of your opt-out may be used in combination with others' information for analytics and modeling purposes.

13. If I've requested that my information not be used for Relevant Mobile Advertising and not used by the AOL Advertising Network, will I still get ads?

Yes, you will receive ads regardless of whether you participate. We expect that the ads you see will be more relevant to you if you are in the program.

14. If I have opted-out of sharing my Customer Proprietary Network Information (CPNI), does that mean I am also opted-out of Relevant Mobile Advertising?

No, the Relevant Mobile Advertising privacy choices are separate from any privacy choices you have made relating to CPNI.

15. If I have already opted-out of the Relevant Mobile Advertising program you described in earlier notices, do I have to opt-out again now that you are combining the program with the AOL Advertising Network?

No, you do not need to register your choice again. Your existing opt-out will remain in place and Verizon Wireless data will not be used in the combined program. You can view your current status and notify us of any changes you may have at www.vzw.com/myprivacy. Note that your opt-out of Relevant Mobile Advertising does not mean that you are opted-out of AOL advertising programs. Please see additional information above in #9.

APPENDIX ATTACHMENT 5

Verizon Wireless' use of a Unique Identifier Header (UIDH)

General Information

1. What advertising programs use the Unique Identifier Header (UIDH)?

Our Relevant Mobile Advertising and Verizon Selects programs help make advertising you see more personalized and useful by using certain customer information we have to connect that advertising with your interests. These advertising programs are part of the AOL Advertising Network and the UIDH is used in these programs.

Details about the data the advertising programs use is available in the FAQs we provide for [Relevant Mobile Advertising](#) and [Verizon Selects](#). Customers can choose whether to be a part of these programs at any time through opt-out (Relevant Mobile Advertising) or opt-in (Verizon Selects) choices found on their privacy settings online, on their device in MyVerizon, or via our toll free number at (866) 211-0874 (for Relevant Mobile Advertising opt-out). Customers also have choices about AOL's use of information it collects and uses for advertising purposes.

We do not share information that identifies you personally as part of these programs other than with vendors and partners who do work for us. We require that these vendors and partners protect the information and use it only for the services they are providing us.

2. What is a UIDH?

Header information is included in all web traffic and includes information such as the device type, preferred language, and content support so that the site receiving the request knows how to best display the site on the phone or other device that sends the request. Verizon Wireless includes a Unique Identifier Header (UIDH), a random string of characters, in the address information that accompanies some of the Internet (http) requests transmitted over our wireless network.

Unless you opt out of the Relevant Mobile Advertising program and have not opted in to the Verizon Selects program, a UIDH is included in the address information of Internet requests going to Verizon companies (including AOL) and a small number of partners to help deliver services unrelated to advertising, such as authentication of devices on our network. In addition, with your opt-in consent, for example when you opt in to the Verizon Selects program, the UIDH may be shared with partners who help provide advertising services. Verizon partners are authorized to use the UIDH only as part of Verizon and AOL services and not for their own separate uses. The UIDH does not contain any personally identifiable data and it does not broadcast individuals' historical web browsing activity to advertisers or others.

3. Why and how is a UIDH used?

The advertising programs use online and device identifiers, including AOL browser cookies, ad IDs from Apple and Google, and the UIDH. The identifiers are used to make our advertising programs better by, for example:

- Linking Verizon advertising program information to information AOL has, to provide more personalized advertising.
- Serving ads to customers in apps and web browsers that do not use common advertising identifiers.
- Helping to determine that different devices have the same user, so AOL can deliver better advertising in more places.
- Determining that an identifier fits into a marketing audience so that the device will receive particular relevant ads.
- Mitigating advertising fraud.
- Ad reporting, modeling and attribution.

The UIDH may also be included in address information of Internet requests going to a small number of Verizon partners to help deliver services unrelated to advertising. For example, the UIDH can be used to authenticate a device as valid on the Verizon network.

Does the UIDH affect my privacy?

The UIDH does not contain any personally identifiable data and it does not broadcast individuals' historical web browsing activity to advertisers or others. Distribution of the UIDH is limited. Unless you opt out of the Relevant Mobile Advertising program and have not opted in to the Verizon Selects program, a UIDH is included in the address information of Internet requests going to Verizon companies (including AOL) and a small number of partners who help deliver services unrelated to advertising, such as authentication of devices on our network. With your opt-in consent, for example when you opt in to the Verizon Selects program, the UIDH may be shared with partners who help provide advertising services. Verizon partners are authorized to use the UIDH only as part of Verizon and AOL services and not for their own separate uses. In addition, other privacy protections are designed into the UIDH, for example, it changes automatically and frequently.

Is the UIDH still present if a customer has opted-out of the advertising programs?

Verizon Wireless will stop inserting the UIDH after a customer opts out of the Relevant Mobile Advertising program or activates a line that is ineligible for the advertising program. Government and

enterprise lines are examples of ineligible lines. The UIDH will still appear for a short period of time after a customer opts out of the Relevant Mobile Advertising program or activates an ineligible line. If a customer chooses to participate in Verizon Selects, the UIDH will be present even if the customer has also opted-out of the Relevant Mobile Advertising program.

APPENDIX ATTACHMENT 6

Business & Marketing Insights

The Business and Marketing Insights program combines and analyzes customer information in a way that does not identify customers personally. The program uses information about how you use your mobile device including web browsing, apps and features you use, and the location of your device, as well as certain information about your Verizon products and services (such as device type) and information we obtain from other companies (such as gender, age range, and interests).

Business and Marketing Insights may be used by Verizon and others who want to better understand customer actions in aggregate. For example, a company could find it valuable to understand the number of customers in different age groups who visited a website, used an app, or visited a retail store or stadium.

Verizon may share location information that does not identify you personally with certain other companies to allow them to produce limited business and marketing insights. For example, de-identified location information we provide could be combined with similar information provided by other wireless carriers to create traffic reports.

See our [Frequently Asked Questions](#) for more information.

You have a choice about whether your information is used in the Business and Marketing Insights program.

Settings	Don't use my information for Business and Marketing Insights	OK to use my information for Business and Marketing Insights
	Select All	Select All
908-229-4103	<input type="radio"/>	<input checked="" type="radio"/>
908-566-8727	<input type="radio"/>	<input checked="" type="radio"/>
312-505-4566	<input type="radio"/>	<input checked="" type="radio"/>
773-485-5273	<input type="radio"/>	<input checked="" type="radio"/>
908-552-5902	<input type="radio"/>	<input checked="" type="radio"/>
908-295-7612	<input type="radio"/>	<input checked="" type="radio"/>

Save Changes

Relevant Mobile Advertising

AOL is now part of Verizon, and we will soon combine Verizon's Relevant Mobile Advertising program into the [AOL Advertising Network](#). These programs use certain customer information to help make the ads you see more interesting and useful.

The Relevant Mobile Advertising program uses your postal and email addresses, certain information about your Verizon products and services (such as device type), and information we get from other companies (such as gender, age range, and interests). The AOL Advertising Network uses information collected when you use AOL Services and visit third-party websites where AOL provides advertising services (such as web browsing, app usage, and location), as well as information that AOL obtains from third-party partners and advertisers.

We do not share information that identifies you personally as part of these programs other than with vendors and partners who do work for us. We require that these vendors and partners protect the information and use it only for the services they are providing us.

These programs use online and device identifiers, including AOL browser cookies, ad IDs from Apple and Google, and one created by Verizon, known as a Unique Identifier Header (or UIDH). When the Verizon and AOL programs are combined, the UIDH will be inserted in certain web traffic that is sent only to Verizon companies (including AOL) and to certain partners who will be authorized to use the UIDH only as part of Verizon and AOL services. More information is available about the [Relevant Mobile Advertising](#) program and the [UIDH](#).

You have a choice about whether to participate in the Relevant Mobile Advertising program. The UIDH discussed above will stop being inserted in web traffic from your device after you opt out of the Relevant Mobile Advertising program, but will still appear for a short period of time after you opt out. Please note that if you opt-out of Relevant Mobile Advertising, but you have opted in to Verizon Selects, you will continue to receive relevant advertising and the UIDH will remain present.

You also have [choices](#) about how AOL uses information for advertising purposes.

Settings	No, I don't want to participate in Relevant Mobile Advertising	Yes, I want to participate in Relevant Mobile Advertising
	Select All	Select All
908-229-4103	<input checked="" type="radio"/>	<input type="radio"/>
908-566-8727	<input type="radio"/>	<input checked="" type="radio"/>
312-505-4566	<input type="radio"/>	<input checked="" type="radio"/>
773-485-5273	<input checked="" type="radio"/>	<input type="radio"/>
908-552-5902	<input checked="" type="radio"/>	<input type="radio"/>
908-295-7612	<input type="radio"/>	<input checked="" type="radio"/>

Save Changes

APPENDIX ATTACHMENT 7

Need Help Ordering? [Chat Now](#) [Call Now](#)



Thank you for your loyalty

VERIZON SMART REWARDS

Choosing Verizon has never been more rewarding. Register and see how fast your rewards points add up just by doing what you already do. Then reward yourself with enticing deals around town or around the world. Plus, enter our sweepstakes by simply logging on or using points for a chance to become one of over 300 winners every day!

[Register for Smart Rewards](#)

Already Registered? [SIGN IN & SHOP >](#)

How Smart Rewards WORKS

1

Register today
YOUR POINTS ARE WAITING

You'll start with 10,000 points and extra points for every year you've been with Verizon.

- You can check your points balance in My Verizon.

[FREQUENTLY ASKED QUESTIONS >](#)

2

Earn points automatically
SEE HOW QUICKLY THEY ADD UP

You'll be amazed at how fast you earn points just for doing things you already do.

- Earn points for every dollar you spend when you pay your bill.
- Get points for paperless billing or setting up Auto Play with your checking account.

[SEE ALL THE WAYS TO EARN POINTS >](#)

[WATCH THIS VIDEO FOR MORE TIPS](#)

3

So many ways to REWARD YOURSELF

From gift cards to deals to savings, there's no telling where your points can take you.

- Redeem points for savings on gift cards to popular department stores, retailers and more.
- Enjoy local deals on dining, shopping and entertainment.
- Save up to 40% on brand name merchandise.
- Get up to 40% off travel worldwide including hotels, cruises & car rentals.

[Register Now](#)

Your REWARDS CENTER


Sweepstakes


Auctions


Daily Deals



Local Deals


Gift Cards


Merchandise


Travel

RESIDENTIAL BUSINESS **WIRELESS**
Overland Park, KS Español Store Locator Contact Us Sign Out


Shop ▾ Support ▾ My Verizon ▾

Register for Verizon Smart Rewards and Verizon Selects

And get even more out of your wireless experience

By joining Verizon Smart Rewards, you also become part of Verizon Selects. You get an extra 2,500 bonus points immediately and another 500 points every month with Verizon Selects. Verizon Selects personalizes the content and marketing you may receive from Verizon and other selected companies.

To continue, please review the Verizon Smart Rewards and Verizon Selects terms and conditions below and select "I Agree" to both.

* Indicates a required field.

Effective Date: July 28, 2014

Verizon Smart Rewards Terms and Conditions

With Verizon Smart Rewards (the "Program"), eligible Verizon Wireless customers can Play, Save and Win. These Terms and Conditions govern your participation in the Program.

You can access the Program through your My Verizon account or My Verizon Mobile application. However, the Program is managed by Destination Rewards, Inc. ("Program Manager"). Destination Rewards, Inc. is not an affiliate of Verizon Wireless. Destination Rewards, Inc. is responsible for Program content, the Program Website and platform, and for the goods, services and gift cards offered as part of the Program, except as limited by these Terms and Conditions. Contact information for the Program

I Agree

Verizon Selects

Verizon Selects aims to enhance your experience by personalizing marketing you may receive from Verizon and other selected companies. To do this, we ask permission to use information about your use of Verizon products and services, the websites you visit and apps you use, as well as your device and its location. We may also use other information like age range, shopping preferences and information about the quantity, type, destination, location, and amount of use of your Verizon voice services (known as CPNI).

We will not share information that identifies you personally with non-Verizon companies. Your CPNI may be shared among Verizon companies. You have a right, and Verizon has a duty, under federal law, to protect the confidentiality of your CPNI.

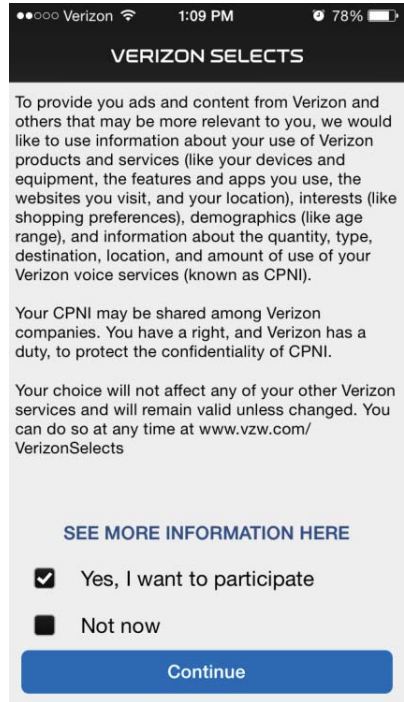
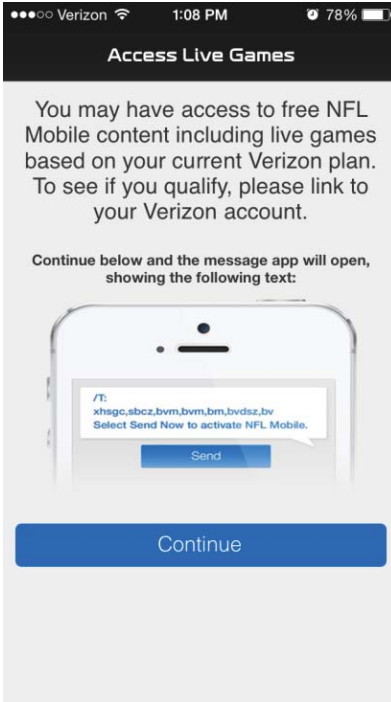
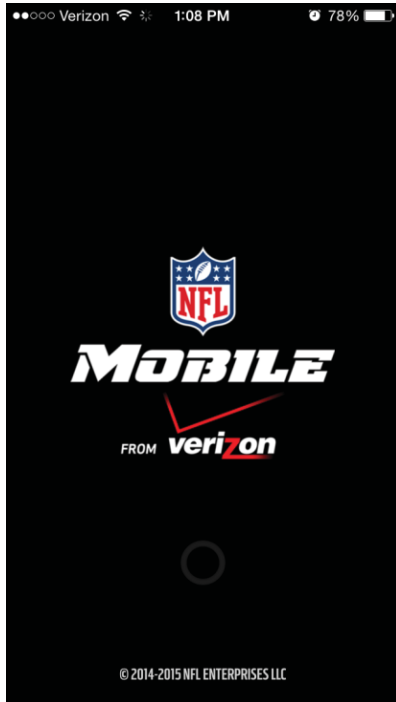
You may grant approval below and your choice will remain in effect until you change it. Update your choice any time in your My Verizon profile or at [vzw.com/verizonselects](#). Your choice here doesn't affect any of your other Verizon products and services.

[See full participation agreement.](#)

I Agree

Cancel Continue

APPENDIX ATTACHMENT 8



APPENDIX ATTACHMENT 9

VERIZON SELECTS PARTICIPATION AGREEMENT

Your privacy is an important priority at Verizon. Our [privacy policy](#) describes the information we collect and how we use it.

This notice provides detail about the Verizon Selects program.

Verizon Selects

The Verizon family of companies, which includes AOL, offers a wide and growing variety of free services, including The Huffington Post, MapQuest, and go90. Like many others online, these services are made possible by advertising. The best advertising is for something you might actually want, and that is what we want to give you.

As part of the AOL Advertising Network, Verizon Selects uses customer information to help make the ads you see more interesting and useful across the devices and services you use or via mail, email or text when you have approved it.

What information is used?

Information used by the Verizon Selects program includes:

- Information about your wireless device including websites you visit, apps and features you use, and device and advertising identifiers
- Information about your device location
- Your postal and email addresses
- Information about the quantity, type, destination, location, and amount of use of your Verizon telecommunications and interconnected voice over internet services and related billing information (also known as Customer Proprietary Network Information or CPNI)
- Information about your Verizon products and services and how you use them (such as data and calling features and use, FiOS service options, equipment and device types)
- Information we get from other companies (such as gender, age range, interests, shopping preferences, and ad responses)

This information may be combined with information the [AOL Advertising Network](#) collects when you use AOL Services and visit third-party websites where AOL provides advertising services (such as web browsing, app usage, and location), as well as information that AOL obtains from third-party partners and advertisers. This information is described in the [AOL privacy policy](#).

We do not share information that identifies you personally in this program other than with vendors and partners who do work for us. We require that these vendors and partners protect the information and use it only for the services they are providing us.

Does the program use device identifiers?

The program uses online and device identifiers, including AOL browser cookies, ad IDs from Apple and Google, and one created by Verizon, known as a Unique Identifier Header or UIDH. Verizon includes a UIDH in the address information of Internet requests going to Verizon companies (including AOL) and to a small number of partners to help deliver services unrelated to advertising. In addition, when you opt in to Verizon Selects, the UIDH may also be shared with partners who provide advertising services. Verizon partners are authorized to use the UIDH only as part of Verizon and AOL services.

We use these identifiers to help make our advertising programs better by, for example:

- Linking Verizon advertising program information to information AOL has, to provide more personalized advertising
- Serving ads to customers in apps and web browsers that do not use common advertising identifiers
- Helping to determine that different devices have the same user, so AOL can deliver better advertising in more places

Your CPNI and other information will be shared among the Verizon family of companies. You have a right, and Verizon has a duty, under federal law, to protect the confidentiality of your CPNI.

Your choices

You must join Verizon Selects to be a part of it, and you can change your mind at any time. You will remain a participant until you withdraw your consent. Information Verizon Selects collects while you are a participant may be kept for up to three years. You can visit the [Verizon Selects Preference Center](#) to learn how to stop participating.

If you choose not to participate, your choice will not affect any of your other Verizon services.

You also have [choices](#) about how AOL uses information for advertising purposes. *Please note that using browser controls such as clearing cookies on your devices or clearing your browser history is **not** an effective way to opt-out of the Verizon or AOL advertising programs.*

If you do not want the UIDH (discussed above) included in any of your web traffic, you should opt out of the separate [Relevant Mobile Advertising program](#) and not opt-in to Verizon Selects.

Additional Information

More information is available about [Verizon Selects](#) and the [Unique Identifier Header](#). The [Verizon](#) and [AOL](#) privacy policies provide additional details about information we collect and how we use it.

APPENDIX ATTACHMENT 10

Verizon Selects FAQs

General Information

1. What is Verizon Selects?

Verizon Selects, part of the [AOL Advertising Network](#), helps make marketing you see more personalized and useful to you across the devices and services you use.

Verizon Selects uses:

- a. Information about your wireless device including websites you visit, apps and features you use, and device and advertising identifiers
- b. Information about your device location
- c. Your postal and email addresses
- d. Information about your Verizon products and services and how you use them (such as data and calling features and use, FiOS service options, equipment and device types). Some of this information is CPNI (Customer Proprietary Network Information), which is information about the quantity, type, destination, location, and amount of use of your Verizon telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information
- e. Information we get from other companies (such as gender, age range, interests, shopping preferences, and ad responses)

This information may be combined with information the AOL Advertising Network collects when you use AOL Services and visit third-party websites where AOL provides advertising services (such as web browsing, app usage, and location), as well as information that AOL obtains from third-party partners and advertisers. This information is described in the [AOL privacy policy](#).

The advertising program uses online and device identifiers including AOL browser cookies, advertising IDs from Apple and Google, and one created by Verizon, known as a Unique Identifier Header or UIDH. Verizon includes a UIDH in the address information of Internet requests going to Verizon companies (including AOL) and to a small number of partners to help deliver services unrelated to advertising, such as authentication of devices on our network. When you opt in to Verizon Selects, the UIDH may also be shared with partners who help us provide advertising services. Verizon partners are authorized to use the UIDH only as part of Verizon and AOL services and not for their own separate uses. More information about the UIDH can be found [here](#).

For more information, watch our "What is Verizon Selects" [video](#).

Review the full [Verizon Selects Participation Agreement](#).

2. What are the benefits of joining Verizon Selects?

In addition to making the ads you see more personalized, you get an extra 2,500 Verizon Smart Rewards bonus points when you first join the program and another 500 points every month for each eligible line on your account that is part of Verizon Selects. To learn more about the Verizon Smart Rewards program, please see the [Smart Rewards FAQs](#).

3. If I participate in Verizon Selects, will you share data that identifies me with non-Verizon companies?

We do not share information that identifies you personally as part of these programs other than with vendors and partners who do work for us. We require that these vendors and partners protect the information and use it only for the services they are providing us.

4. Will the advertising program use information obtained from accessing or reading my emails or texts?

No, information will not be obtained from reading the content of your emails or texts.

5. Where will I see advertising?

You'll see ads in the same places you see them today, such as on websites and in apps on the devices you use or via mail, email or text when you have approved it.

6. What types of devices will receive advertisements?

Devices you have on your Verizon Wireless account and those you use to log in to My Verizon will receive ads. In addition, you may receive advertising on devices you use to connect directly to AOL sites and services, or on third party sites where AOL provides advertising services. If you share your mobile hotspot with others, ads relevant to you may also appear on other connected devices.

7. What types of accounts may participate?

Consumer and small business customers may participate in Verizon Selects. Corporate or government accounts aren't eligible to participate. Certain other lines may also be ineligible (e.g., lines that an Account Owner has requested be blocked from participation).

8. How can I join Verizon Selects?

You can learn more about how to participate by visiting the [Verizon Selects Preferences Center](#) in My Verizon and following the prompts to opt in.

9. If I provided my consent to participate in Verizon Selects, and then I turn off the location-based services settings on my mobile device, will my location information still be collected and used for Verizon Selects?

Yes, Verizon Selects uses location information that Verizon collects from our network and is not related to the location settings on your device. If available, Verizon Selects also may use location information collected from your mobile device. If you do not want the advertising program to use your location information, you can withdraw your consent at any time by visiting the [Verizon Selects Preference Center](#).

You can also instruct Verizon to stop using past data it has collected about your web browsing and location to direct ads in the Verizon Selects program by visiting the [Verizon Selects Preference Center](#). Information previously collected may continue to be used in combination with others' information for analytics and modeling purposes.

AOL and Verizon also offer apps and other services that involve the collection of location information from your device (for example, MapQuest). When you turn off location based services on your device or use other device controls, the ad programs will not receive location information from these apps. AOL may also use location information provided by advertisers themselves. More details can be found in the [AOL Supplemental Mobile Terms of Service and Privacy Policy](#).

10. If I provide my consent, how long will you keep and use my data for Verizon Selects?

You will remain a participant in Verizon Selects until you withdraw your consent. Information Verizon Selects collects while you are a participant may be kept for up to three years.

11. What kind of choices do I have as to whether my information is used for Verizon Selects?

We won't use your information for Verizon Selects unless you provide your consent by opting in. Once you have decided to participate in Verizon Selects, you can visit the [Verizon Selects Preference Center](#) to:

- Instruct Verizon to stop using past data it has collected about your web browsing and locations to direct ads in the Verizon Selects program. Information previously collected may continue to be used in combination with others' information for analytics and modeling purposes.
- Disable other lines on your account from participating if you are the account owner or account manager.
- Stop participating in Verizon Selects.

If I decide to participate in Verizon Selects now, can I change my mind later?

Yes, you can do so at any time by visiting the [Verizon Selects Preferences Center](#).

How will I know that my Verizon Selects choices have been processed?

When you make a choice or modify an existing one from the [Verizon Selects Preferences Center](#), a confirmation message will display after your choices are saved. You can also view your current status.

Do I have choices about being part of the AOL Advertising Network?

You have [choices](#) about how AOL uses your information for advertising purposes. You can opt-out of receiving interest-based ads when you browse the web by visiting the [Digital Advertising Alliance's consumer choice](#) page and selecting "AOL Advertising." This opt-out choice will apply only to the browser you are using when you opt-out, so if you are using multiple browsers or devices, you will need to repeat this process on each. Please note that blocking or deleting cookies in your browser may cancel your choice to opt-out.

You can make your opt-out choice apply to any browser you use while signed into AOL by adjusting your [AOL Marketing Preferences](#).

You can also opt-out of receiving advertisements targeted to your mobile device using the "Limit Ad Tracking" or similar capability on your device or by following the instructions provided at this [Mobile Device Choices](#) page.

Can I opt-out of these advertising programs by deleting my browser cookies?

No, using browser controls such as clearing cookies on your device or clearing your browser history is **not** an effective way to opt-out of the Verizon and AOL advertising programs. Instead, if you want to opt-out, you should take the steps outlined above.

I have added my phone number to the Federal Do Not Call registry, or have told Verizon that I don't want to receive certain kinds of marketing, such as mail, emails or phone calls. How do these choices affect my participation in Verizon Selects?

Your decision to participate in Verizon Selects is independent of any other choices you've made previously.

APPENDIX ATTACHMENT 11

Verizon Selects



Click to view what is Verizon Selects video

Get 2,500 Smart Rewards points MANAGE VERIZON SELECTS

Receive messages and offers with Verizon Selects. Join today and you may be eligible to earn 2,500 Smart Rewards points for signing up and 500 points per line every month, redeemable for daily deals, vacation getaways and more.

[Learn about Verizon Smart Rewards](#)

*separate registration required for Verizon Smart Rewards

What is Verizon Selects?

Verizon Selects helps to personalize the advertising you receive across the devices you use. When you join Verizon Selects, you also receive more Smart Rewards points to use. For more information, click here to see the [Verizon Selects FAQs](#).

Start earning more points today!

You can earn additional Smart Rewards Points every month for each line on your account which participates in Verizon Selects. We've made it easy for you. Click here to select the lines you want Verizon to send a text invitation to on your behalf.



Manage your preference Settings for 949- [REDACTED]

Web Browsing and Location Data for Verizon Selects

The data we use for Verizon Selects helps us tailor the marketing messages you receive so they are more personalized. You can request Verizon to stop using the Verizon Selects program past data it has collected about your web browsing and location. Information previously collected may still be used in combination with others' information for analytics and modeling purposes.

Verizon Selects Data	<input type="checkbox"/> Reset Verizon Selects web browsing and location history
----------------------	--

Verizon Selects Participation Status

Verizon Selects Status	Active since 11/19/12	<input type="checkbox"/> Withdraw Consent
------------------------	-----------------------	---

[Review the full Verizon Selects Participation Agreement](#)

APPENDIX ATTACHMENT 12

Business and Marketing Insights FAQs

General Information

1. What are business and marketing insights?

Business and marketing insights are observations about groups or categories of Verizon Wireless customers. Insights developed in this program do not identify you personally. For example, a company may find it valuable to know the number of customers in different age groups who visited a website, used an app, or visited a retail store or stadium.

2. Will I ever be personally identified in a business and marketing insight?

No, insights are developed about groups or categories of customers and do not identify you personally.

3. What kind of data is used to prepare business and marketing insights?

Information used by the Business and Marketing Insights program includes:

- Information about your wireless device including websites you visit, apps and features you use, and device and advertising identifiers
- Information about your device location
- Information about your Verizon products and services and how you use them (such as data and calling features and use, equipment and device types)
- Information we get from other companies (such as gender, age range, and interests)

The Business and Marketing Insights program combines and analyzes this information in a manner that does not identify you personally to prepare insights for use by Verizon and others. Verizon may also share location information in a way that does not personally identify you so that others can produce limited business and marketing insights. For example, de-identified location information we provide could be combined with similar information provided by other wireless carriers to create traffic reports.

Will Verizon Wireless read my emails or collect my private information from my online bank account (or other online accounts where I register to perform secure transactions) to prepare these business and marketing insights?

No.

What types of accounts and devices are included in the development of business and marketing insights?

Most Verizon Wireless consumer and small business accounts are included in the development of business and marketing insights. This includes mobile phones, tablets, mobile hotspots, netbooks and USB modems. Corporate, government and prepaid accounts are not included.

What is the purpose of business and marketing insights?

Business and Marketing Insights may be used by Verizon and others who want to better understand customer actions in aggregate. For example, a company could find it valuable to understand the number of customers in different age groups who visited a website, used an app, or visited a retail store or stadium.

If I turn off the location-based services (LBS) settings on my mobile device, will my location information still be collected and used for business and marketing insights?

Yes, the location information that Verizon collects from our network is not related to the location settings on your device. If available, we may also use location information collected from your mobile device. If you don't want us to use your location information to develop these insights, you can opt-out by visiting the [privacy choices](#) page in My Verizon or by calling (866) 211-0874. If you have a multi-line account, you should indicate your privacy choice for each individual line.

Can I refuse permission to use my information for business and marketing insights?

Yes, if you don't want us to use your information to develop business and marketing insights, you can tell us by visiting the [privacy choices](#) page in MyVerizon or by calling (866) 211-0874. If you have a multi-line account, you should indicate your privacy choice for each individual line. Also, please note that this opt-out does not include any reporting or insights developed as part of AOL Advertising programs.

If I decide to allow you to use my information for business and marketing insights, can I change my mind later?

Yes, you can change your privacy choices at any time.

Will the Business and Marketing Insights program share my personal information with third parties?

We do not share information that identifies you personally as part of this program other than with vendors and partners who do work for us. We require that these vendors and partners protect the information and use it only for the services they are providing us.

If I have opted-out of sharing my Customer Proprietary Network Information (CPNI), does that mean I am also opted-out of Business and Marketing Insights?

No. The Business and Marketing Reports privacy choices are separate from any privacy choice you have made relating to CPNI.

APPENDIX ATTACHMENT 13

Relevant Online Advertising Program

What is Relevant Online Advertising?

The Relevant Online Advertising program helps advertisers reach Verizon Online customers with offers, coupons, and incentives that may be better tailored to their interests. Because the online ads can be directed to you based on information about your address, demographics and interests, and certain information about the Verizon products and services you have, the ads you receive with the Relevant Online Advertising program may be more relevant to you. This program was previously called Digital Direct Marketing.

What information will Verizon use to make online ads more relevant to me?

The information we use includes the postal address we have for you and certain consumer information about your Verizon products and services (such as broadband and video features) as well as demographic and interest categories provided to us by other companies (such as gender, age range, sports fan, frequent diner, or pet owner). Verizon won't share information that identifies you personally with advertisers as part of this program. You can learn about Verizon's ad practices by visiting Verizon's [Privacy Policy](#)

Here's an example: A local restaurant may want to advertise only to people who live within 10 miles and tend to be frequent diners, and we might help deliver that ad on a website without sharing information that identifies you personally.

Does the program use my Web activity?

No, the Relevant Online Advertising program does not use information about the particular websites you visit.

Does this program use location information?

Yes, the program uses your postal address.

Is any of my personal information shared?

We do not share information that identifies you personally as part of these programs other than with vendors and partners who work for us. We require that these vendors and partners protect the information and use it only for the services they are providing us. Verizon won't share any information that identifies you personally with advertisers as part of this program.

How will I see Relevant Online Advertising?

You'll see ads on the websites you visit in the same way you see them today; however, some of the ads may be more relevant to you. For example, a business using our program could offer coupons and promotions for products or services based on your address, your interests or demographics, or your Verizon products and services.

If I decide to allow Verizon to use my information for Relevant Online Advertising, can I change my mind later?

Yes, you can change your privacy choices at any time by going to the **My Services** area of **My Verizon**, click on **Internet**, then click on **Manage** and select the **Manage Online Advertising Preferences** link.

Can I choose not to participate in Relevant Online Advertising?

Yes, you can choose not to participate. Go to the **My Services** area of **My Verizon**, click on **Internet**, then click on **Manage** and select the **Manage Online Advertising Preferences** link.

If I choose not to participate, will I still see online ads?

The program does not increase the amount of advertising you receive. The websites you visit will provide the same number of ads whether you choose to participate or not. If you choose not to participate, you may still receive website ads that are delivered using other technologies unrelated to this program. Visit Verizon's [Privacy Policy](#) for more information on our advertising practices. If you would like to find out more information about online advertising (including your choices about other forms of targeted online ads), you can visit the advertising industry-sponsored website, aboutads.info.

If I have opted-out of sharing my Customer Proprietary Network Information (CPNI), does that mean I am also opted-out of Relevant Online Advertising?

No. The privacy choices for the program are separate from any privacy choices you have made relating to CPNI. In order to make your selections specifically for Relevant Online Advertising, go to the **My Services** area of **My Verizon**, click on **Internet**, then click on **Manage** and select the **Manage Online Advertising Preferences** link.