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

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

REPLY COMMENTS OF THE
UNITED STATES TELECOM ASSOCIATION

The United States Telecom Association (USTelecom)[1] is pleased to submit its reply comments in response to the Commission's Notice of Proposed Rulemaking ("Notice")[2] proposing a new privacy regime for broadband Internet access service (BIAS) providers. In the Notice, the Federal Communications Commission (Commission) seeks comment on its application of traditional privacy requirements of the Communications Act of 1934, as amended ("the Act") to BIAS providers in order to close what the Commission sees as a gap between the current FTC privacy regime and FCC jurisdiction over ISPs under Title II of the Communications Act.[3]

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives – all providing advanced communications service to both urban and rural markets. USTelecom members provide a full array of services, including broadband, voice, data and video over wireline and wireless networks.

[2] *See Notice of Proposed Rulemaking, FCC, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* WC Docket No. 16-106, FCC 16-39 (rel. Apr. 1, 2016) (*Notice*).

[3] *Id.* at ¶1.

In this proceeding hundreds of comments have been filed and a majority of those are voices in opposition to the FCC's proposal as overbroad. One of the exceptions is an effort led by Public Knowledge in conjunction with The Benton Foundation, Consumer Action, Consumer Federation of America and National Consumers League (collectively, PK),[4] which has been very vocal in combating industry efforts to continue providing broadband service in an open and innovative way. As such, USTelecom focuses our reply comments on issues raised in PK's comments in this proceeding.

PK bases its arguments in favor of overly strict privacy regulation on ISPs on two major fallacies: first that BIAS providers as ISPs are the gatekeepers to information about how consumers use the Internet and, second, that forcing an opt-in regime on consumers will benefit consumer welfare.

As to the first fallacy, PK asserts it in the first sentence of their comments[5] then repeats it throughout 39 pages to argue that because of that one concept (which is wrong) consumers should fear their ISPs and FCC privacy regulations should not be harmonized with the FTC because an "FTC-style" approach is not feasible.[6] PK tries to ignore the data presented in Peter Swire's paper[7] by saying that predictive analytics in advertising is a newer more effective

[4] See Comments of Public Knowledge, The Benton Foundation, Consumer Action, Consumer Federation of America, and National Consumers League, WC Docket No. 16-106 (filed May 27, 2016) (PK Comments).

[5] *Id.*

[6] PK Comments at 24.

[7] *See Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others,* A Working Paper of The Institute for Information Security & Privacy at Georgia Tech, Peter Swire, Associate Director, The Institute for Information Security & Privacy, Huang Professor of Law Georgia Tech Scheller College of Business and Senior Counsel, Alston & Bird LLP, Justin Hemmings, Research Associate, Georgia Tech Scheller College of Business

approach to targeted marketing being used by companies that somehow negates the pertinence of Mr. Swire's research.[8] In fact predictive analytics is a technique that has been used by all sorts of advertisers for years and there has never been increased risk to privacy rights or other harm shown. The technique is not new nor does it trump Swire's data, in particular, because of the continued prevalence of encryption. As the Association of National Advertisers (ANA) points out in its comments, "the FCC has not established a record of consumer harm that necessitates new regulation in this area or justifies the specific approach put forward by the FCC. In fact, the current online ecosystem subsidizes content and programming that consumers value, promotes innovation, and grows the economy."[9] As evidence ANA includes a recent study commissioned by Direct Marketing Association's (DMA) Data-Driven Marketing Institute (DDMI), titled, "The Value of Data: Consequences for Insight, Innovation, & Efficiency in the U.S. Economy," which quantifies the concrete economic benefits of data. This study found that the Data-Driven Market Economy (DDME) generates vital revenue and jobs for the U.S. economy and that the use of data-driven marketing added $202 billion in revenue to the U.S. economy and fueled more than

---

and Policy Analyst, Alston & Bird LLP & Alana Kirkland, Associate Attorney, Alston & Bird LLP (Feb. 29, 2016) (*Swire Paper*).

[8] PK Comments at 6-11.

[9] Comments of the Association of National Advertisers, WC Docket No. 16-106 (filed May 27, 2016) at 1-2, *citing*, a recent Zogby Analytics poll commissioned by the Digital Advertising Alliance ("DAA") shows that consumers assign a value of almost $1,200 a year to ad-supported online content. DAA, Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth $1,200/Year; 85% Prefer Ad-Supported Internet to Paid, PR Newswire (May 11, 2016 8:30 AM), http://www.prnewswire.com/news-releases/zogby-poll--americans-say-free-ad-supported-online-services-worth-1200year-85-prefer-ad-supported-internet-to-paid-300266602.html (ANA Comments).

966,000 jobs in 2014.[10] The study also found that the U.S. DDME provides the American people with high value jobs.[11] Therefore not only are advertisers already using responsible data practices including self-regulation,[12] the unnecessary new restrictions in the Commission's NPRM could threaten these economic benefits.

PK says that, "failure to account for the rise of predictive analysis fatally undermines the central thesis of Swire's argument,"[13] and refers to a letter summarizing the debate between Nick Feamster and Peter Swire[14] as evidence of this fact. While the letter does lay out the foundation for the debate between the two professors including a debate about the role of predictive analytics, PK fails to acknowledge that at the conclusion of the letter – approved of by both parties – it states that Feamster agrees with Swire in large part, and authorized him to include the following: "Upon more careful review of the paper, I have not found anything in the report that I believe is incorrect."[15] This is hardly a fatal blow to Swire's paper, or a legitimate basis for dismissing Swire's work.

PK also argues that the data collected by BIAS providers is commercially valuable in and of itself in 2 ways: (1) providers blend it with unique information obtained from non-internet services like set top box info and (2) providers have unique info about use of devices in the home that edge providers do not have.[16] In attempting to demonstrate this, PK gives an example of

---

[10] *See Id.*

[11] *Id.* at 1-2.

[12] *Id.* at 3-5.

[13] PK Comments at 9.

[14] https://peterswire.net/wp-content-uploads/feamster-siwre-final.pdf.

[15] *See Id.*

[16] PK Comments at 12.

how a user can go to Google to search for a Fitbit, but then goes to Amazon.com to purchase it, and those independent actions are trivial and not valuable.[17] However, if an ISP knows that the consumer went to Google and Amazon, but due to encryption has no idea what the consumer searched for on those sites, those visits for which no substance can be seen is somehow valuable.[18] If, as PK asserts, that in the world of predictive analytics "no fact is considered too trivial or too far afield,"[19] then why are ISPs being singled out? The plain fact is that regardless of how valuable isolated bits of information may be when combined with others, it cannot be that they are proprietary to only one type of provider but not others. For example, IP addresses are not proprietary information or CPNI and should not be treated as such under the FCC's rules.[20]

A substantial portion of internet traffic is encrypted now, and,[21] as the Swire Paper points out encryption will reach the 70% level by the end of this year.[22] In fact there is overwhelming evidence that encryption adoption increases every day.[23] PK's back-up argument is that even if the site is encrypted ISPs still see IP addresses which they believe is valuable information. They also quote a 2010 article that posits that even encrypted information is often leaked due to

---

[17] *Id.* at 12-13.

[18] *Id.* at 13.

[19] *Id.* at 8.

[20] See Comments of CTIA, WC Docket No. 16-106 (filed May 26, 2016) at 44 (CTIA Comments); Comments of AT&T Services, Inc., WC Docket No. 16-106 (filed May 27, 2016) at 75-78 (AT&T Comments); Comments of Comcast Corporation, WC Docket No. 16-106 (filed May 27, 2016) at 77-81 (Comcast Comments).

[21] PK Comments at 17.

[22] *Swire Paper* at 29, *citing*, 2016 Global Internet Phenomena, Spotlight: Encrypted Internet Traffic," Sandvine, Feb. 2016.

[23] *Id.*

failures in web based applications that allow an eavesdropper to infer sensitive information.[24] It is curious that PK provides no evidence in its comments to suggest this is true or at the very least that what may have been reported in an article in 2010 is even still the case in 2016.

The reality is that the theory that ISPs have comprehensive and unique access to, and knowledge about, users' online activity and that ISPs derive this information from their role in connecting consumers to the Internet is outdated. Technological developments have placed substantial limits on ISPs' visibility into consumer data and online activities, while other Internet companies often have access to far more information and a wider range of user information than ISPs because they are able to collect consumer information in many different ways (i.e., search queries, operating systems, browsers, social networks, online commerce sites, etc.). There clearly can be no "comprehensive" ISP visibility into user activity when an ISP today is the conduit for only a fraction of a typical user's online activity and ISP visibility into user activity continues to decline.

By contrast, Internet companies that are not ISPs have long been able to gather information about online user activity from multiple services and platforms, such as: (1) social networks; (2) search engines; (3) webmail and messaging; (4) operating systems; (5) mobile apps; (6) interest-based advertising; (7) browsers; (8) Internet video; and (9) e-commerce. For example, with respect to search engines, when the search is performed over an HTTPS connection, as has become the norm, the ISP can only see which search engine was used and the host domain (website) of the clicked link, but not the search query or the full URL (webpage) that was clicked.

[24] PK Comments at 21, *citing*, Shuo Chen et al., *Side Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow*, Proceedings 2010 IEEE Symp. On Security & Privacy 191 (2010) http://research.microsoft/pubs/119060/WebAppSideChannel-final.pdf.

PK also argues that multiple device usage increases not decreases the granularity of data that BIAS provider can collect on its users because multiple apps are set to sync across devices and the home ISP has the ability to see what the user is doing regardless of the network the user is using.[25] However in reality, as consumers use more devices and locations to access their social networks, webmail, and e-commerce sites, a growing share of advertising tracking targets the user across multiple devices. Today, "cross-device" and "cross-context" data collection and use is dominated by non-ISPs. Further, unlike many websites, ad networks and other online entities that may have only ephemeral contacts with the consumers from whom they collect data, ISPs have an ongoing business relationship with their customers, which creates strong, built-in incentives to safeguard the privacy of their subscribers and further mitigates against subjecting ISPs to heightened privacy obligations.

PK's second major fallacy is that consumers are somehow better served by a regime that forces them to make decisions about opting-in to sharing even their least sensitive information. As Dr. Wright points out in his declaration, sharing information produces very substantial consumer welfare gains and opt-out regimes for non-sensitive information are likely to best align with maximizing consumer welfare PK says that the FTC privacy framework supported by the industry is a "by type" privacy regime that regulates only especially sensitive data that can't possibly work in the broadband ISP context.[26] PK fails to understand that the FTC model for privacy protection has already been working in the broadband ISP context for some time. Moreover, the FTC regime is not merely a "by type" regime because it does not only protect

[25] PK Comments at 17-19.

[26] PK Comments at 24-26.

sensitive information.[27] The FTC seeks to protect all information under framework of whether disclosure of that information would be unfair or deceptive.[28] This framework allows carriers to take into consideration the context in which the data will be used, thus allowing for consumers to get access to advertising and information that they would reasonably expect to get from their provider, and allow for continued innovation. PK counters that the only way to ensure information is protected is to overreach and ensure ALL information is protected.[29] All of this fails to take into account that ISPs already protect their users' personal information and will continue to do so[30] and that the FTC's privacy framework has been in effect in the context of broadband ISPs for years and it has been successful.

PK also falls back on another argument that the Commission has been relying on in this proceeding – that the consumer must be sole ruler of his or her information.[31] PK states quite aptly that because "consumer preferences in this realm are not static or even uniform"[32] consumers should be the ones in charge of their information. USTelecom does not dispute that consumers do know what is important to them with regard to what personal information should be considered private and what shouldn't, however the FCC's proposed opt-in regime is an overreach to achieve the goal of giving consumer's control over their personal information.

---

[27] *Protecting Consumer Privacy in an Era of Rapid Change* at 56 (March 2012), 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 Privacy Report*).

[28] *Id.* at 15-16.

[29] PK Comments at 24.

[30] See Comcast Comments at 38-40; Comments of the National Cable & Telecommunications Association, WC Docket No. 16-106 (filed May 27, 2016) at 50-52 (NCTA Comments).

[31] PK Comments at 27-33.

[32] PK Comments at 27.

Such an approach will only serve to stifle innovation and the dissemination of useful information to consumers creating the economic harm that ANA speaks of.[33]

Instead of allowing a system that already works continue to flourish, PK would like to take a step backwards and calls for the Commission to even further expand its proposed opt-in approach to all information including telecommunications-related services and affiliate services[34] because it says that the burden of protecting a user's information must fall on the provider not the consumer. PK warns that such a move is necessary because of what it calls "inevitable arbitrage." PK explains that this arbitrage is what it sees as the unguarded potential for the broadband industry to adopt a "total service" approach to broadband wherein BIAS providers will attempt to sweep in all sorts of services to attempt to have it covered under the communications related services opt-out.[35] Here, once again, PK is fantasizing about potential behavior that is not based on any facts. The FTC approach which has governed the ISP industry for years has been successful. There is no real or imagined harm that needs to be fixed. In fact, it is precisely the type of sensible privacy regime that has allowed the broadband industry to flourish in the way that it has. It seems that PK is simply advocating to remove all advertising on the internet such that the broadband industry and the conveniences it provides to consumers would be sent back into the dark ages. Furthermore, should an ISP participate in behavior that could be defined as arbitrage, it would fall under the purview of the FTC's ban on harmful and deceptive regime and be thwarted in that way. Ultimately, a broad opt-in consent mechanism would only serve to hamper an ISP's ability to compete with the edge providers that dominate

[33] *See supra* at 3.

[34] PK Comments at 28-31.

[35] PK Comments at 30-31.

online advertising, and therefore imposing substantial costs on ISPs that ultimately would trickle down to consumers.[36]

PK says that in the alternative, should the FCC maintain the opt-out regime for telecommunications-related services, it should circumscribe it as narrowly as possible because of this threatened "arbitrage."[37] Possible and unfounded threats of arbitrage are simply conjecture and fear mongering. PK does this in other parts of its comments by throwing in a red herring about the use of the data for purposes of discrimination.[38]

PK makes the argument that with AT&T's program low income consumers would be forced to choose between privacy rights or no broadband connection at all,[39] but provides no detail at all to back up that assertion. What PK fails to understand is that the exchange of information that is used for advertising purposes for discounted or free products and services, also known as the ad-supported business model, is common in the Internet ecosystem. Furthermore it has underwritten the Internet's development such that it has grown and thrived into its current form. Removing these sorts of opportunities for consumers would only prove to be economically harmful to them.[40]

---

[36] Comcast Comments at 52-57; Comments of the Direct Marketing Association, WC Docket No. 16-106 (filed May 27, 2016) at 17-19 (DMA Comments); Comments of Verizon, WC Docket No. 16-106 (filed May 27, 2016) at 34-36 (Verizon Comments).

[37] PK Comments at 31.

[38] PK Comments at 15-17.

[39] PK Comments at 32.

[40] See AT&T Comments at 2; ANA Comments at 5-11.

The Commission should step back and truly analyze all of the comments and data filed in this proceeding for their fact-based merits. The Commission is attempting to fix a problem that does not exist using an erroneous conclusion as a starting point. Instead the Commission should look carefully at the FTC framework and harmonize its new rules with those time-tested policies.

Respectfully submitted,

UNITED STATES TELECOM ASSOCIATION

By: _____

B. Lynn Follansbee
Jonathan Banks
Its Attorneys

607 14th Street, NW, Suite 400
Washington, D.C. 20005
202-326-7300

July 6, 2016