



*Before the*  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC, 20554

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

**COMMENTS OF CONSUMER WATCHDOG**

**MAY 27, 2016**

With the reclassification of Broadband Internet Access Service (BIAS) providers under Title II of the Communications Act as common carriers, the Commission took on the legal obligation under Section 222 to protect the privacy of broadband subscribers. Without explicit FCC regulations, there is a dangerous vacuum because the Federal Trade Commission by law has no jurisdiction over common carriers. The Commission must enact robust privacy rules as rapidly as possible, not only to protect consumers from serious violations of their privacy by ISPs, but also to bring certainty to the BIAS providers as to what they are – and are not – allowed to do. Some in the industry have argued for delaying this proceeding, but that makes no sense. Consumers and providers are both best served by clarity and certainty regarding the rules of the road for the information superhighway.

Consumer Watchdog<sup>1</sup> applauds the Commission for this rulemaking to enact regulations covering BIAS providers that protect Customer Personal Information (CPI), which includes

---

<sup>1</sup> Consumer Watchdog is a nonprofit organization dedicated to educating and advocating on behalf of consumers for over 25 years. Its mission is to provide an effective voice for the public interest. Consumer Watchdog's programs health care reform, oversight of insurance rates, energy policy, protecting privacy rights, protecting legal rights, corporate reform, and political accountability. [www.consumerwatchdog.org](http://www.consumerwatchdog.org).

Customer Proprietary Network Information (CPNI) and Personally Identifiable Information (PII). Section 222 clearly gives the Commission the authority to promulgate privacy regulations covering ISPs, and developing those rules quickly is imperative. Section 706 also provides additional authority to protect privacy with appropriate regulations on BIAS providers. Unless consumers are assured that they have control over their data, their trust in the Internet will falter, likely undermining their use of broadband. If subscribers believe that their privacy is compromised and are less inclined to use broadband, Section 706 requires the Commission to take steps to rectify the problem, in this case by enacting privacy protecting regulations.

### **Consumers Have Broad And Justifiable Concerns About Privacy On The Internet**

Not all consumer privacy concerns about the Internet are focused on BIAS providers. As the results from a recent Pew Survey<sup>2</sup> found:

- Ninety-one percent of adults agree or strongly agree that they have lost control of how personal information is collected and used by companies.
- Americans express a consistent lack of confidence about the security of everyday communication channels and the organizations that control them.
- Few adults are confident that the records of their activities maintained by various companies and organizations, including phone companies, email providers and cable companies, will remain private and secure.
- Large majorities of adults view as sensitive information their Social Security numbers, the state of their health, the content of their phone conversations, emails and text messages, their physical locations over time, the numbers they have called or texted, their birth dates, their relationship histories, the websites they have visited, and the searches they have made.
- Seventy-four percent of adults say that it is very important for them to be able to control who gets information about them and 65 percent say it is very important for them to control who can collect information about them.

---

<sup>2</sup> Lee Rainie, *The state of privacy in America: what we learned*, Pew Research Center, January 20, 2016, <http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/>

- Many Americans struggle to understand the nature and scope of data collected about them. Forty-seven percent said they did not know how their information would be used, and many of these people felt confused, discouraged or impatient when trying to make decisions about sharing their personal information with companies.
- Eighty-six percent of Internet users have taken steps to mask their digital footprints, and many say they would like to do more but don't know how.
- Some 68 percent of Internet users believe current rules are not strong enough in protecting people's privacy online; and 64 percent believe the government should do more to regulate advertisers. Most expect at least some limits on retention policies by data collection firms.

As the Pew results demonstrate, it is not just BIAS providers that prompt people's privacy concerns. It is the entire Internet ecosystem. The invasive privacy practices of edge providers like Google and Facebook raise huge concerns because they collect much of the same personal data as ISPs. That is why in June 2015 Consumer Watchdog petitioned<sup>3</sup> the Commission to use its Section 706 authority to begin a rulemaking that would require edge providers to honor do-not-track requests sent from a consumer's web browser. The Wireline Competition Bureau, acting on behalf of the Commission, declined the petition, saying, "The Commission has been unequivocal in declaring that it has no intent to regulate edge providers."<sup>4</sup>

Requiring that edge providers honor do-not-track requests is an important regulatory protection with a very limited impact on them. It brings transparency to the Internet ecosystem in that consumers now don't even know if their do-not-track (DNT) requests are being honored. (In most cases, they are not.) Such a requirement would increase consumer trust in the Internet, prompting greater broadband use and deployment. The Commission could and should exercise its ancillary authority under Section 706 to enact a DNT regulation. Consumer Watchdog continues to urge you do to so at the appropriate time. However, we understand that the focus of

---

<sup>3</sup> Consumer Watchdog's Petition to FCC, June 15, 2015, <http://www.consumerwatchdog.org/resources/fccdntpetition061515.pdf>

<sup>4</sup> FCC Denial of Consumer Watchdog Petition, Nov. 6, 2015, <https://www.fcc.gov/document/bureau-dismisses-petition-regulate-edge-provider-privacy-practices>

this NPRM is Section 222 privacy regulations and we offer comments on those important and necessary proposed rules.

### **BIAS Providers Have Unique Power to Monitor and Intrude Into Consumers' Lives**

Pervasive collection and exchange of personal data, without meaningful privacy protections, has become the norm across much of the Internet. Nonetheless, BIAS providers occupy a unique spot in the Internet ecosystem. They have access to virtually all of a subscriber's Internet traffic. Even if the data is encrypted, a great deal is revealed purely from basic header information such as IP addresses, ports, and timing.<sup>5</sup> A BIAS provider can paint a detailed composite portrait of a user's life. Edge providers gather data when a consumer uses their services or visits a website that does. To a limited extent, if an edge provider's practices are unacceptable, a consumer can opt not to use the service. Such choices don't work with a BIAS provider. Your ISP sees everything. It knows where you went, when you went there and how long you stayed. Such data can be very revealing. Frequent visits to Disney's site indicate children in the household. Visits to various health related sites reflect details about the user's health. The ISP is in a unique position to amass deeply revealing personal profiles, share the data with third parties or use it for its own purposes.

While a consumer can opt not to visit a particular edge provider (though avoiding Google is nearly impossible), once they chose an ISP they are more or less locked into that choice because of the difficulties in changing to another provider. Exacerbating the situation is the fact that most ISPs exercise monopolistic power in their respective markets.<sup>6</sup>

Broadband providers are not shy about describing how they scrape and misuse their subscribers' data. As the Center for Digital Democracy's Jeffrey Chester discusses at great length in a recent

---

<sup>5</sup> See, e.g., Tech. Analysis Branch, Office of the Privacy Comm'r of Can., What an IP Address Can Reveal About You (2013), [https://www.priv.gc.ca/information/research-recherche/2013/ip\\_201305\\_e.pdf](https://www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.pdf) (noting wide range of information that may be discerned from an IP address).

<sup>6</sup> Rickard Greenfield, *Fortune*, "How the cable industry became a monopoly," May 19, 2015, <http://fortune.com/2015/05/19/cable-industry-becomes-a-monopoly/>

white paper<sup>7</sup>, major BIAS providers regularly highlight the invasiveness and ubiquity of their tracking schemes in order to market the data they collect.

***Consumers Must Have Control of Their Data; Consent Must Be Opt-In***

There is a longstanding understanding in the world of traditional telephones that customer information gathered by virtue of the subscriber's use of the network cannot be used for any other purpose without the subscriber's permission. This same principle must apply to the BIAS provider's network. The subscriber's information belongs to the subscriber, and they must have control of whether and how it is used. In addition to CPNI gathered through the network, BIAS providers have access to other PII. Both must be protected and the consumer should be granted control over how it is used. Consumer Watchdog believes the Commission's approach of giving illustrative, non-exhaustive guidance on what constitutes PII (data that can be linked to an individual) and CPNI (data that is gathered about the subscriber from the network) is correct. Moreover, the examples detailed in the NPRM are useful.

Once the consumer subscribes to a BIAS provider, they understand that they have given permission to use data necessary to operate the network. But they have not given any consent for their PII or CPNI to be used for any other purpose. Clearly ISPs have a strong incentive to use the data for other, commercial purposes.

How should they seek the subscriber's permission? All consent should be explicit, informed consent and provided on an opt-in basis. The burden must be on the BIAS provider to clearly explain how the consumer's data will be used and to make the case why it should be allowed.

Consent should be sought on a just-in-time basis, just before the BIAS provider proposes to use the data. The ability to withdraw consent after it had been given should be consistently and readily available.

---

<sup>7</sup> Jeff Chester, Center for Digital Democracy, "Big Data is Watching: Growing Digital Data Surveillance of Consumers by ISPs and Other Leading Video Providers," 23 Mar. 2016, <https://www.democraticmedia.org/article/big-data-watching-growing-digital-data-surveillance-consumers-isps-and-other-leading-video>

Opt-out consent is insufficient. In fact, it is not really consent. Opting-out places the burden on consumers to take extra steps to avoid something that likely was not adequately explained to them. Consumers have difficulty exercising opt-out choice because they don't have the same level of knowledge as the data holder about exactly how their personal information may be used. In addition they may make erroneous assumptions about their rights or the companies' practices.<sup>8</sup> Opt-in consent should be required for all additional uses and sharing of a consumer's data.

When a BIAS provider collects data, consumers must be assured that the information is secure. Meaningful policies limiting data retention should be in place and any stored customer data should be required to be encrypted.

### ***Pay-For-Privacy Policies Are Coercive; Must Be Limited***

Some ISP's are offering discounts to consumers who share their data. Consumer Watchdog believes such "pay-for-privacy" policies can rapidly become coercive and predatory, especially when applied to lower-income subscribers. Pay-for-privacy schemes are most likely to have a negative impact on minority communities, low-income neighborhoods and the elderly. If widely adopted, they would create a two-tiered system, in which only the wealthy will be able to protect their privacy. This is unfair; fundamental privacy protections must be made available at no cost to all broadband users. New research "reveals most Americans do not believe that 'data for discounts' is a square deal." Ninety-one percent disagree (77 percent of them strongly) with the argument that "if companies give me a discount, it is a fair exchange for them to collect information about me without my knowing."<sup>9</sup> The Commission must ensure that abusive and coercive pay-for-privacy practices that take unfair advantage of consumers are not allowed.

### ***No "Multi-stakeholder Process"***

The NPRM asks whether the Commission should incorporate a so-called "multi-stakeholder" process into its commendable efforts to protect consumers' privacy. The Department of

---

<sup>8</sup> See Chris Jay Hoofnagle and Jennifer M. Urban, Berkeley Law, *Alan Westin's Privacy Homo Economicus*, 19 Wake Forest L. Review 261 (2014),

<http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3399&context=facpubs>.

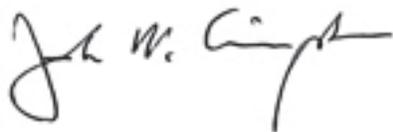
<sup>9</sup> Joseph Turow, Ph.D., Annenberg School of Communication, University of Pennsylvania; Michael Hennessy, Ph.D., Annenberg Public Policy Center; Nora Draper, Ph.D., University of New Hampshire, *The Tradeoff Fallacy*, June 2015 [https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy\\_1.pdf](https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf).

Commerce conducted three such proceedings aimed at developing codes of conduct to protect privacy for mobile apps, facial recognition and unmanned aircraft systems. The FCC should not convene such proceedings. The Department of Commerce's efforts have not been effective. The proceedings were largely captured by industry and produced codes with little significant impact. Indeed, consumer and privacy advocates were so disappointed with the facial recognition proceeding that they withdrew.<sup>10</sup> The FCC has rulemaking authority and should exercise it appropriately. There is no useful purpose to a "multi-stakeholder" process.

### **Conclusion**

Consumers must have control of their data and how it is used and shared. The Commission's rulemaking focused on BIAS providers, especially if the opt-in model for consent is adopted, will provide important privacy protections covering an important section of the Internet ecosystem. Further action in the future by the Commission to ensure that edge providers comply with privacy protections will also be necessary.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "John M. Simpson". The signature is fluid and cursive, with a long horizontal stroke at the end.

John M. Simpson  
Privacy Project Director

---

<sup>10</sup> Elizabeth Weise, *USA Today*, "Privacy Groups Leave Over Dispute on Facial Recognition Software," June 6, 2015, <http://www.usatoday.com/story/tech/2015/06/16/facial-recognition-software-google-facebook-moments-ntia/28793157/>