

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)
)
CONSUMER WATCHDOG) RM: _____
)
Petition for Rulemaking to Require Edge)
Providers to Honor 'Do Not Track' Requests)
)

**PETITION FOR RULEMAKING TO REQUIRE EDGE PROVIDERS TO HONOR 'DO
NOT TRACK' REQUESTS**

John Simpson, Privacy Project Director
Laura Antonini, Counsel
CONSUMER WATCHDOG
2701 Ocean Park Blvd., Ste. 112
Santa Monica, CA 90405
Telephone: (310) 392-0522
Facsimile: (310) 392-8874

June 15, 2015

TABLE OF CONTENTS

I. SUMMARY.....1

II. BACKGROUND.....3

A. Section 222 and its Implementing Regulations Evidence Congress’s and the Commission’s Commitment to Protecting Consumer Privacy.....3

B. The Commission’s Enforcement Bureau is Actively Protecting Consumers’ Privacy Through Enforcement Actions.....5

C. Providers of Broadband Internet Access Service Are Now Covered by Section 222..6

D. The Commission Intends to Open a Rulemaking Proceeding to Adopt Rules Governing CPNI in the Broadband Internet Access Service Context.....7

E. People Are as Concerned About Privacy-Invasive Practices – Such as Online Tracking – by Edge Providers as They Are Those by Broadband Internet Access Service Providers.....9

III. NEED FOR RULEMAKING.....11

A. Edge Providers Are Under No Obligation to Honor ‘Do Not Track’ Requests.....11

B. The Commission Found Broadband Deployment in the United States is Failing to Keep Pace and Must Take Immediate Action.....13

IV. THE COMMISSION HAS THE AUTHORITY TO PROMULGATE THE PROPOSED RULE UNDER TITLE I OF THE ACT AND SECTION 706 OF THE TELECOMMUNICATIONS ACT OF 1996.14

V. PROPOSED RULE17

VI. CONCLUSION.....18

I. SUMMARY

Consumer Watchdog hereby petitions the Federal Communications Commission to initiate a rulemaking proceeding requiring “edge providers” (like Google, Facebook, YouTube, Pandora, Netflix, and LinkedIn) to honor “Do Not Track” Requests from consumers.

Consumers should have a right to keep their personal information private. Companies should be prevented from tracking personal information and web activity without consumers’ knowledge and permission. The Commission recognized the importance of protecting consumers’ information online in its 2015 Open Internet Order.¹

The Commission’s 2015 Open Internet Order reclassified broadband Internet access service as a telecommunications service under Title II of the Communications Act of 1934, emphasizing the importance of protecting consumer privacy by finding “that if consumers have concerns about the privacy of their personal information, such concerns may restrain them from making full use of broadband Internet access services and the Internet, thereby lowering the likelihood of broadband adoption and decreasing consumer demand.”² It was for this reason that the Commission decided to apply Title II’s Section 222 to broadband Internet access service providers. Section 222 makes clear that telecommunication carriers have the duty of protecting CPNI, with particular emphasis on privacy concerns for personal, individualized data.³

However, the Commission decided to forbear from application of the Commission’s current CPNI regulations to broadband Internet access service providers, since the regulations that were intended to apply to telephone services do not reflect technological differences and

¹ *In the Matter of Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, FCC 15-24 (Mar. 12, 2015) (“2015 Open Internet Order”).

² *Id.* at para. 464.

³ 47 U.S.C. § 222 *et seq.*

advances between broadband and telephone services. Thus the Commission created a temporary gap in privacy protections. The Commission acknowledged this gap by stating its intent to promulgate CPNI rules in the broadband context in a separate proceeding. On April 28, 2015, the Commission held a public workshop on broadband consumer privacy, which Commission Chairman Tom Wheeler called the “beginning of a very important conversation.”⁴

It is imperative for the protection of consumers that this conversation include regulation of edge providers, which provide “content, applications, services, and devices accessed over or connected to broadband Internet access service[.]”⁵ Consumers’ privacy concerns about the Internet extend far beyond the broadband providers who are impacted by Section 222. Many consumers are as concerned – or perhaps even more worried – about the online tracking and data collection practices of edge providers. Because activities by edge providers pose the same threat to widespread broadband adoption as any privacy practice of broadband Internet access service providers, the Commission should, in addition to the CPNI rules it intends to adopt, promulgate rules protecting the unauthorized use of consumers’ personal information by requiring edge providers to honor “Do Not Track” Requests.

⁴ FCC, *Public Workshop on Broadband Privacy* at 6:54 (Apr. 28, 2015), <https://www.fcc.gov/events/wcb-and-cgb-public-workshop-broadband-consumer-privacy>.

⁵ *In the Matter of Preserving the Open Internet Broadband Industry Practices*, GN Docket No. 09-191, WC Docket No. 07-52, Report and Order, FCC 10-201, para. 20 (Dec. 23, 2010).

PETITION FOR RULEMAKING TO REQUIRE EDGE PROVIDERS TO HONOR ‘DO NOT TRACK’ REQUESTS

Pursuant to Sections 1.401 and 1.1 of the Commission’s rules,⁶ Consumer Watchdog⁷ respectfully petitions the Commission to initiate a rulemaking proceeding to require edge providers to honor “Do Not Track” Requests under its “ancillary jurisdiction” under Title I of the Act,⁸ and its duty to “encourage the deployment on a reasonable and timely basis of advanced telecommunications” and “take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition” under Section 706 of the Telecommunications Act of 1996.⁹

II. BACKGROUND

A. *Section 222 and its Implementing Regulations Evidence Congress’s and the Commission’s Commitment to Protecting Consumer Privacy.*

With the passage of Section 222 of the Act¹⁰ Congress clearly demonstrated its intention to protect the privacy of information that telecommunications service¹¹ providers gain about their

⁶ 47 C.F.R. §§ 1.1, 1.401.

⁷ Consumer Watchdog is a nonprofit, nonpartisan consumer advocacy organization with offices in California and Washington, D.C., specializing in the application of state and federal consumer protection laws. Founded in 1985, Consumer Watchdog advocates for the rights of consumers and seeks to hold corporations accountable in the legislature and the courts. One of Consumer Watchdog’s chief missions is to protect consumers’ privacy rights. Through policy research, consumer education, media advocacy, and legal action, Consumer Watchdog has focused new and substantial attention on the issue of online privacy, calling out some of the most egregious violators and prompting strong action by regulators. Consumer Watchdog, and the public on whose behalf Consumer Watchdog advocates, are vitally interested in ensuring that consumers are protected from the harm caused by corporations that collect and use their personal information online.

⁸ 47 U.S.C. §§ 151 *et seq.*; *see, e.g.*, 47 U.S.C. § 154(i) (“[t]he Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions”).

⁹ 47 U.S.C. § 1302(a), (b).

¹⁰ 47 U.S.C. § 222.

customers by virtue of them using the provider’s network, by imposing a duty on all telecommunications carriers “to protect the confidentiality of proprietary information of ... customers[.]”¹²

Congress enacted Section 222 to “ ‘define[] three fundamental principles to protect all consumers. These principles are: (1) the right of consumers to know the specific information that is being collected about them; (2) the right of consumers to have proper notice that such information is being used for other purposes; and (3) the right of consumers to stop the reuse or sale of that information.’ ”¹³

CPNI¹⁴ receives the highest level of privacy protection under the Act.¹⁵

Telecommunications carriers that collect CPNI must adhere to strong rules under the Act and the Commission’s regulations to protect consumers’ privacy.¹⁶

¹¹ 47 U.S.C. § 153(53) defines “telecommunications service” as “the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.” A “telecommunications carrier” is “any provider of telecommunications services, except that such term does not include aggregators of telecommunications services (as defined in section 226 of this title).” *Id.* at §153(51).

¹² 47 U.S.C. § 222(a). Section 222 requires telecommunications service providers to protect customer data shared with the service provider solely as a result of the provision of that service, requires consent before carriers may use, disclose, or permit access to consumer information, and affords customers the right to inspect their own information. 47 U.S.C. § 222(b)-(c).

¹³ *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Declaratory Ruling, FCC 13-89, para. 10 and fn. 16 (Jun. 27, 2013) (quoting H.R. Conf. Rep. No. 458, 104th Cong., 2d Sess. 204 (1996) (Joint Explanatory Statement of the Committee of Conference)).

¹⁴ *See* 47 U.S.C. § 222(h)(1)(A) (CPNI is “information that related to the quantity, technical configuration, type, destination, location and amount of use of a telecommunication service subscribed to by any customer”).

¹⁵ 2015 Open Internet Order at para. 462.

¹⁶ Under the regulations: a telecommunications carrier cannot use CPNI for marketing purposes unless it receives a customer’s permission; nor can it share CPNI with a third party without

B. *The Commission’s Enforcement Bureau is Actively Protecting Consumers’ Privacy Through Enforcement Actions.*

The Commission is increasingly meeting its statutory commitment to protecting privacy through strong enforcement actions regulating privacy breaches and violations of CPNI rules. For example, on April 8, 2015, AT&T agreed to pay a \$25 million civil penalty for its failure “to properly protect the confidentiality of almost 280,000 customers’ proprietary information, including sensitive personal information such as customers’ names and at least the last four digits of their Social Security numbers and CPNI in connection with data breaches at AT&T call centers in Mexico, Columbia, and the Philippines.”¹⁷ Within a week of the AT&T fine, the Commission “joined the Asia Pacific Privacy Authorities (APPA), the principal international forum for privacy enforcement authorities in the Asia Pacific Region.”¹⁸

Also, in October 2014, the Commission announced its “intent to fine phone carriers TerraCom and YourTel \$10 million for several violations of laws protecting the privacy of phone customers’ personal information.”¹⁹ The companies “apparently stored Social Security numbers, names, addresses, driver’s licenses, and other sensitive information belonging to their customers on unprotected Internet servers that anyone in the world could access.”²⁰ And in September 2014, the Commission reached a \$7.4 million settlement with Verizon to address the company’s

permission; permission for use of the information by the carrier for marketing purposes may be based on opt-out approval; and permission to share CPNI with an unaffiliated third party requires explicit opt-in consent. 47 U.S.C. § 222(a), (c)(1); 47 C.F.R. §§ 64.2001 – .2011.

¹⁷ *In the Matter of AT&T Services, Inc.*, File No.: EB-TCD-14-00016243, Order, DA 15-399 (Apr. 8, 2015).

¹⁸ Press Release, FCC, FCC Joins Asia Pacific Privacy Authorities (Apr. 15, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-333037A1.pdf.

¹⁹ Press Release, FCC, FCC Plans \$10 Million Fine For Carriers That Breached Consumer Privacy (Oct. 24, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-330136A1.pdf.

²⁰ *Id.*

unlawful marketing of its phone and other services to two million customers without their consent or notification of their privacy rights.²¹

The Commission's privacy actions have not been limited to phone carriers. In 2012, the Commission fined Google \$25,000 for deliberately impeding and delaying its investigation of Google's collection of personal e-mails, text messages and other communications from private Wi-Fi networks as its cars traveled streets for its Street View location service.²²

C. *Providers of Broadband Internet Access Service Are Now Covered by Section 222.*

On March 12, 2015, the Commission released the text of the 2015 Open Internet Order establishing new net neutrality rules applicable to providers of broadband Internet access service.²³ In addition to new rules governing the conduct of broadband Internet access providers,²⁴ the Commission reclassified broadband Internet access service as a "telecommunications service." This reclassification means that providers are now considered common carriers under Title II of the Act.²⁵

²¹ Press Release, FCC, Verizon To Pay \$7.4 Million To Settle Consumer Privacy Investigation (Sept. 3, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-329127A1.pdf.

²² See *In the Matter of Google, Inc.*, File No. EB-10-IH-4055, Notice of Apparent Liability for Forfeiture, DA 12-592 (Apr. 13, 2012), http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0416/DA-12-592A1.pdf.

²³ The Commission defines "broadband Internet access service" as: "A mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this Part." 2015 Open Internet Order at para. 25.

²⁴ These rules, which will apply equally to both fixed and mobile broadband providers, prohibit blocking, throttling, and paid prioritization, require enhanced transparency, and govern future conduct by broadband Internet access providers. 2015 Open Internet Order. The 2015 Open Internet Order also declared mobile broadband to be a commercial mobile service. *Id.*

²⁵ Title II of the Act allows the Commission to place strict "common carrier" regulations on

While the Commission has the ability to forbear from applying sections of Title II when it is in the public interest to do so, particularly in light of technological advances, the Commission wisely decided to apply Section 222 of the Act to broadband Internet access service providers. The 2015 Open Internet Order states:

As the Commission has recognized, “[c]onsumers’ privacy needs are no less important when consumers communicate over and use broadband Internet access than when they rely on [telephone] services.” Thus, this Order finds that consumers concerned about the privacy of their personal information will be more reluctant to use the Internet, stifling Internet service competition and growth. Application of section 222’s protections will help spur consumer demand for those Internet access services, in turn “driving demand for broadband connections, and consequently encouraging more broadband investment and deployment,” consistent with the goals of the 1996 Act.^[26]

The 2015 Open Internet Order is the Commission’s response to the decision in *Verizon v. Federal Communications Commission*, 740 F.3d 623 (2014) (“*Verizon*”), where the U.S. Court of Appeals for the District of Columbia held that the Commission’s previous net neutrality rules failed because they treated broadband Internet access service providers as if they were common carriers, a characteristic of telecommunication services rather than “information services”²⁷ as they were classified at that time.

D. *The Commission Intends to Open a Rulemaking Proceeding to Adopt Rules Governing CPNI in the Broadband Internet Access Service Context.*

Although the Commission applied Section 222 to broadband Internet access providers,

“telecommunications services.” Common carrier regulations can include requirements that providers offer their services to all customers, that those services be offered at reasonable prices, and that providers refrain from discriminating in the provision of those services. *See* 47 U.S.C. §§ 201 *et seq.*

²⁶ 2015 Open Internet Order at para. 54.

²⁷ The Act defines “information service” as “the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications . . . but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.” 47 U.S.C. § 153(24).

“the Commission declined to apply current privacy regulations under Section 222 to [broadband providers].”²⁸ The Commission did not apply the Commission’s regulations to broadband Internet access services because the regulations were developed to apply to phone service and “questions about the application of those privacy requirements can arise and must be dealt with by the Commission as technology evolves[.]”²⁹ For example, the Commission cited “customers’ web browsing history” as an instance of sensitive information not covered by current CPNI rules.³⁰ The Commission promised “a separate rulemaking proceeding” to adopt “rules to govern broadband Internet access service[.]”³¹ On April 28, 2015, the Commission held a workshop to discuss how Section 222’s protections would apply to broadband providers after the 2015 Open Internet Order.³²

The Commission’s Enforcement Bureau issued a Public Notice on May 20, 2015 providing “guidance to broadband providers about how the Enforcement Bureau intends to enforce Section 222 in connection with “broadband services during this time when no rules have been promulgated.”³³ The Commission stated that “the Enforcement Bureau intends to focus on whether broadband providers are taking reasonable, good-faith steps to comply with Section 222, rather than focusing on technical details.”³⁴ The Enforcement Bureau stated it will provide “informal as well as formal guidance to broadband providers as they consider how best to

²⁸ 2015 Open Internet Order at para. 467.

²⁹ *Id.* at para. 466.

³⁰ *Id.* at para. 467.

³¹ *Id.* at para. 462.

³² FCC, Public Workshop on Broadband Privacy, Apr. 28, 2015, <https://www.fcc.gov/events/wcb-and-cgb-public-workshop-broadband-consumer-privacy>.

³³ FCC, Public Notice, *Enforcement Advisory No. 2015-03*, DA 15-603 (May 20, 2015), <https://www.fcc.gov/document/isps-should-take-reasonable-steps-protect-privacy>.

³⁴ *Id.*

comply with Section 222.”³⁵ The Enforcement Bureau’s actions are certainly a move in the right direction, but a rulemaking broadly addressing control of personal information online is now necessary to protect consumers’ privacy.

E. *People Are as Concerned About Privacy-Invasive Practices – Such as Online Tracking – by Edge Providers as They Are Those by Broadband Internet Access Service Providers.*

While the eventual promulgation of robust CPNI rules governing broadband Internet access service providers may ease some privacy concerns, the fact is that consumers are concerned about the privacy practices of edge providers³⁶ like Google, Facebook, Amazon, YouTube, LinkedIn, and Pandora. Consumers worry about being tracked as they surf the Web and are concerned about the digital dossiers that are built about them and their activities often without their knowledge and consent.

A recent Pew Research Center poll found:

Americans feel privacy is important in their daily lives in a number of essential ways. Yet, they have a pervasive sense that they are under surveillance when in public and very few feel they have a great deal of control over the data that is collected about them and how it is used. Adding to earlier Pew Research reports that have documented low levels of trust in sectors that Americans associate with data collection and monitoring, the new findings show Americans also have exceedingly low levels of confidence in the privacy and security of the records that are maintained by a variety of institutions in the digital age.

³⁵ *Id.* Broadband providers can also seek advisory opinions as to whether their conduct is consistent with the 2015 Open Internet Order. *Id.*

³⁶ The Commission has described an “edge provider” as one that “provid[es] content, applications, services, and devices accessed over or connected to broadband Internet access service (‘edge’ products and services).” *In the Matter of Preserving the Open Internet Broadband Industry Practices*, GN Docket No. 09-191, WC Docket No. 07-52, Report and Order, FCC 10-201, para. 20 (Dec. 23, 2010). The *Verizon* court described, “Edge providers are those who, like Amazon or Google, provide content, services, and applications over the Internet[.]” *Verizon* at 629.; *see also* 2015 Open Internet Order at para. 341 (“providers today market and offer consumers separate services that are best characterized as (1) a broadband Internet access service that is a telecommunications service; and (2) ‘add-on’ applications, content, and services that are generally information services”).

While some Americans have taken modest steps to stem the tide of data collection, few have adopted advanced privacy-enhancing measures. However, majorities of Americans expect that a wide array of organizations should have limits on the length of time that they can retain records of their activities and communications.^{37]}

The poll found: “93% of adults say that being in control of *who* can get information about them is important” and “90% say that controlling *what* information is collected about them is important[.]”³⁸

Such doubts and concerns about the privacy of one’s personal information certainly have a negative impact on Internet use and consequently widespread and rapid broadband adoption, as the Commission concluded in its 2015 Broadband Progress Report.³⁹

The public’s fears are justified. Indeed, Google deliberately hacked around default settlings in Safari and placed tracking cookies on consumers’ computers in order to serve targeted ads to users, resulting in a \$22.5 million fine levied by the Federal Trade Commission.⁴⁰

³⁷ Mary Madden and Lee Ranie, *Americans’ Attitudes About Privacy, Security and Surveillance*, Pew Research Center (May 20, 2015), <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.

³⁸ *Id.*; In 2014, the Pew Research Center poll found that: 91% of adults in the survey “agree[d]” or “strongly agree[d]” that consumers have lost control over how personal information is collected and used by companies, and 61% of adults “disagree[d]” or “strongly disagree[d]” with the statement: “I appreciate that online services are more efficient because of the increased access they have to my personal data.” Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center (Nov. 12, 2014), <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>.

³⁹ *In the Matter of Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*, GN Docket No. 14-126, 2015 Broadband Progress Report and Notice of Inquiry on Immediate Action to Accelerate Deployment, FCC 15-10, paras. 104-06 (Feb. 4, 2015) (“2015 Broadband Progress Report”), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-10A1.pdf.

⁴⁰ Google recently paid a civil penalty of \$22.5 million over charges that it “misrepresented to users of Apple Inc.’s Safari Internet browser that it would not place tracking ‘cookies’ or serve targeted ads to those users, violating an earlier privacy settlement between the company and the

Fines are insufficient to protect consumers' privacy from edge providers like Google and Facebook, which ignore consumer privacy concerns as the companies rake in astounding amounts of revenue from their collection of users' personal information.⁴¹

III. NEED FOR RULEMAKING

A. *Edge Providers Are Under No Obligation to Honor 'Do Not Track' Requests.*

The four most popular Web browsers in the United States – Google's Chrome, Mozilla's Firefox, Apple's Safari and Microsoft's Internet Explorer – all offer users the option of sending a Do Not Track message.⁴² By default, the Do Not Track option is not enabled in all four browsers, and must be actively chosen by a user in a browser's preferences.⁴³ Because a user must decide to select the preference, Do Not Track is deemed a clear statement of the user's choice.⁴⁴

Even though all four major browsers can send the Do Not Track message, an edge provider is under no obligation to honor the request. Most do not.⁴⁵

[Federal Trade Commission] FTC." Press Release, Google Will Pay \$22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser, Federal Trade Commission (Aug. 9, 2012), <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented>; *see U.S. v. Google Inc.* (N.D. Cal., Nov. 16, 2012, CV 12-04177 SI) 2012 WL 5833994, at *1.

⁴¹ "Google generated approximately \$58.7 billion from advertising alone in 2014, based on its ability to deliver targeted ads. Facebook also generated most of its \$12.4 billion in revenue last year from targeting ads based on the interests and personal data of its users." Fred Campbell, *Privacy Concerns About Verizon-AOL Deal Are Really Concerns About Increased Competition*, Forbes.com (May 18, 2015), <http://www.forbes.com/sites/realspin/2015/05/18/privacy-concerns-about-verizon-aol-deal-are-really-concerns-about-increased-competition/>.

⁴² *See* Wikipedia, Do Not Track, http://en.wikipedia.org/wiki/Do_Not_Track (last modified April 16, 2015).

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ *See, e.g.*, Google Chrome's help page states, "You can include a 'Do Not Track' request with your browsing traffic. However, many websites will still collect and use your browsing data to improve security, provide content, services, ads and recommendations on their websites, and generate reporting statistics." Google, *Choose your privacy settings*, <https://support.google.com/chrome/answer/114836?hl=en> (last visited May 26, 2015); Google,

Currently, a consumer does not know if his or her expressed Do Not Track request will be honored. This can have two results. First, a consumer can be lulled into believing their data is protected when it is not. Second, if the consumer digs deeper and learns that an edge provider has no obligation to honor the request, it will undermine the consumer's trust in the Internet ecosystem, likely having the detrimental impact on Internet use that has led the Commission to the measures set forth above to protect privacy.

The Worldwide Web Consortium (W3C)'s⁴⁶ Tracking Protection Working Group has been working to develop a Do Not Track standard for more than four years.⁴⁷ The W3C's envisioned standard has two components: (1) the Tracking Preference Expression (TPE) portion, which would standardize the technical aspects of how a Do Not Track message is sent from a web browser to an information service, and (2) the Tracking Compliance and Scope (TCS) portion, which would define the obligations of a website that receives a Do Not Track message.⁴⁸ Even if the W3C publishes a Do Not Track standard, implementation would be completely voluntary.⁴⁹ Clearly, additional action is needed to formalize protections that are not voluntary.

Do Not Track, <https://support.google.com/chrome/answer/2790761?hl=en> (last visited May 26, 2015) (“At this time, most web services, including Google’s, do not alter their behavior or change their services upon receiving Do Not Track requests”).

⁴⁶ The World Wide Web Consortium (W3C) is an international community of “[m]ember [o]rganizations, a full-time staff and the public work[ing] together to develop [w]eb [s]tandards.” W3C, About W3C, <http://www.w3.org/Consortium/> (last visited May 26, 2015). “The W3C mission is to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web.” W3C, W3C Mission, <http://www.w3.org/Consortium/mission>, (last visited May 22, 2015).

⁴⁷ See Thomas Roessler, *Do Not Track at W3C*, W3C (Feb. 24, 2011), <http://www.w3.org/blog/2011/02/do-not-track-at-w3c/>.

⁴⁸ See, e.g., Tracking Compliance and Scope, W3C (Mar. 31, 2015), <http://www.w3.org/TR/tracking-compliance/>

⁴⁹ W3C, Tracking Protection Working Group, <http://www.w3.org/2011/tracking-protection/> (last visited May 22, 2015).

Do Not Track requests – if required to be honored – give consumers increased control over their data and would build trust in the Internet and spur broadband use. A Do Not Track mechanism would allow consumers to tell edge providers that the consumers’ Internet activities should not be tracked. Consumers’ control of their data would be greatly increased, easing concerns about privacy. A rule requiring that Do Not Track signals be honored would undoubtedly put to rest many consumers’ privacy concerns about the Internet. It would certainly bolster broadband deployment and use.

B. *The Commission Found Broadband Deployment in the United States is Failing to Keep Pace and Must Take Immediate Action.*

Section 706 of the Telecommunications Act of 1996 requires the Commission to report annually on whether broadband “is being deployed to all Americans in a reasonable and timely fashion,” and to take “immediate action” if it is not. The 2015 report found that “broadband is not being deployed to all Americans in a reasonable and timely fashion.”⁵⁰

Acting to ensure consumers’ privacy while they use the Internet is one of the immediate steps the Commission should take to bolster the rate of broadband adoption. “As the Commission has found previously, the protection of customers’ personal information may spur consumer demand for those services, in turn ‘driving demand for broadband connections, and consequently encouraging more broadband investment and deployment’ consistent with the goals of the 1996 Act.”⁵¹

⁵⁰ See 2015 Broadband Progress Report at para. 4.

⁵¹ 2015 Open Internet Order at para. 464 (citations omitted).

IV. THE COMMISSION HAS THE AUTHORITY TO PROMULGATE THE PROPOSED RULE UNDER TITLE I OF THE ACT AND SECTION 706 OF THE TELECOMMUNICATIONS ACT OF 1996.

The Commission has authority to adopt rules governing edge providers, as “information services,” pursuant to its authority under Title I of the Act and its duty under Section 706 to “encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans (including, in particular, elementary and secondary schools and classrooms) by utilizing, in a manner consistent with the public interest, convenience, and necessity ... measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment” and to “take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition.”⁵²

Edge providers, which provide online content, applications, and services,⁵³ offer

⁵² The Commission has authority under Title I to promulgate regulations that are shown to be “reasonably ancillary” to the performance of another of the Commission’s statutorily obligated duties. *See Verizon* at 631-32 (describing the Commission’s “ancillary jurisdiction”: “a power that flows from the broad language of Communications Act section 4(i)”). *See* 47 U.S.C. § 154(i) (“The Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions.”); *see generally American Library Ass’n v. FCC*, 406 F.3d 689, 700–03 (D.C.Cir.2005). We have held that the Commission may exercise such ancillary jurisdiction where two conditions are met: ‘(1) the Commission’s general jurisdictional grant under Title I covers the regulated subject and (2) the regulations are reasonably ancillary to the Commission’s effective performance of its statutorily mandated responsibilities.’ *American Library Ass’n*, 406 F.3d at 691–92.’” Here, the two prongs set forth in *Verizon* are met: first, the subject of the regulation is covered by the Commission’s general grant of jurisdiction under Title I of the Communications Act, which encompasses “ ‘all interstate and foreign communication by wire or radio.’ ” *See* 47 U.S.C. § 152(a). Second, consistent with the *Verizon* court’s finding that the Commission had reasonably interpreted Section 706 to be an independent grant of authority upon which the Commission could base regulatory action (*Verizon* at 635-42), Section 706 grants the Commission authority to promulgate a ‘Do Not Track’ regulation “tailored to the specific statutory goal of accelerating broadband deployment—is not so broad that we might hesitate to think that Congress could have intended such a delegation.” *Id.* at 642.

⁵³ The Commission has described an “edge provider” as one that “provid[es] content,

“information services” under the statutory definition. An “information service” is:

the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications . . . but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.^{54]}

Edge providers offer Internet users the capability to generate, acquire, store, transform, process, retrieve, utilize, and make available information via telecommunications, broadband Internet access service. For example: when a Facebook user posts a comment or photograph to her profile, she is generating, storing and making available information via the Internet; Netflix users are acquiring, retrieving, utilizing, and processing information when they stream video content on their laptops; anyone who performs a Google search is generating and acquiring information in their search results; Yahoo! Mail offers users the ability to generate and store information, emails.⁵⁵ These providers are thus offering “information services” under the Act.

Consistent with the Commission’s reasoning in its 2015 Open Internet Order, ensuring consumer privacy will ensure the openness of the Internet and the ability of consumers to access all the legal content and applications of their choice, which will drive consumer demand for broadband Internet access.⁵⁶ The increased demand for services will, therefore, lead to greater

applications, services, and devices accessed over or connected to broadband Internet access service (‘edge’ products and services).” *In the Matter of Preserving the Open Internet Broadband Industry Practices*, GN Docket No. 09-191, WC Docket No. 07-52, Report and Order, FCC 10-201, para. 20 (Dec. 23, 2010). The *Verizon* court described, “Edge providers are those who, like Amazon or Google, provide content, services, and applications over the Internet[.]” *Verizon* at 629.

⁵⁴ 47 U.S.C. § 153(24).

⁵⁵ The Commission has described “cloud-based storage services” and “email” as “information services.” *See* 2015 Open Internet Order, para. 376.

⁵⁶ 2015 Open Internet Order at para. 464.

infrastructure investment⁵⁷ *not only on the part of broadband providers but also on the part of edge providers offering information services*. In turn, increased investment will lead to greater deployment and increased capacity for all Americans, in fulfillment of Section 706(a).⁵⁸

Furthermore, edge providers collect the same sensitive personal information that broadband Internet access service providers collect, and that the Commission is committed to protecting. If the Commission does not act to regulate the collection of personal information by edge providers, the Commission will in effect be granting a regulatory advantage to the edge providers, implicating concerns of market distortions.⁵⁹ In order to maintain regulatory parity, the Commission must impose some rules on edge providers that protect consumers' personal information.⁶⁰

⁵⁷ *Id.*; *see id.* at para. 51 (The Commission found that Section 222 applied to broadband providers, stating that the 2015 Open internet Order “finding ‘that consumers concerned about the privacy of their personal information will be more reluctant to use the Internet, stifling Internet service competition and growth.[] Application of section 222’s protections will help spur consumer demand for those Internet access services, in turn “driving demand for broadband connections, and consequently encouraging more broadband investment and deployment,” consistent with the goals of the 1996 Act.”)

⁵⁸ *See id.*

⁵⁹ AT&T claims it is being placed at a disadvantage as a result of the new rules, including Section 222: “[T]hese added requirements put AT&T at a competitive disadvantage against companies with which it competes to offer services, but which are not subject to these same requirements (because they are not broadband Internet access providers).” *In the Matter of Protecting and Promoting the Open Internet*, Joint Petition for Stay of United States Telecom Association, CITA – The Wireless Association, AT&T Inc., Wireless Internet Service Providers Association, and Centurylink, GN Docket No. 14-28 at p. 27 (May 1, 2015).

⁶⁰ As one former chief of the Commission’s wireless bureau writes, “Google and Facebook are now attempting to entrench their dominance over Internet advertising by arbitraging this new jurisdictional split over online privacy. ... Google and Facebook have strong incentives to preserve their ability to collect personal information online while denying their competitors the same opportunities. The jurisdictional split created by the [2015 Open Internet Order] enables them to achieve this discriminatory result while maintaining a false veneer of consumer protection.” Fred Campbell, *Privacy Concerns About Verizon-AOL Deal Are Really Concerns About Increased Competition*, Forbes.com (May 18, 2015),

V. PROPOSED RULE

Consumer Watchdog petitions the Commission to initiate a rulemaking proceeding to require edge providers to honor users' "Do Not Track" requests, generally containing the provisions set forth below:

"Do Not Track" Request. Under the proposed rule, a "Do Not Track" Request means any signal by a consumer, by any technology or means of communication, to an edge provider that the provider may not "track" his or her personal information. Online "tracking" of personal information should be defined to include, but not be limited to, activities such as collecting, retaining, storing, sharing, selling, or using a consumer's personal information over time and across a third-party online service or services.

Personal Information. The proposed rule should define "personal information" to include, but not be limited to, traditionally identifying information as well as information about a consumer's online activity, such as:

- a name, a postal address or other location, an email address or other username, a telephone or fax number, a government-issued identification number, such as a tax identification number, a passport number, or a driver's license number, an account number, credit card or debit card number, or any required security code, access code, or password that is necessary to permit access to a consumer's financial account;
- Internet websites and content from Internet websites accessed, the date and hour of online access, the computer and geo-location from which online information was accessed, and the means by which online information was accessed, such as, but not limited to, a device, browser, or application;
- any unique or substantially unique identifier that can lead to the real-time identification of a single user or device, such as a customer number or Internet Protocol address;
- and any other information that could be used to identify, or is associated with, a particular consumer, including but not limited to biometric information.

<http://www.forbes.com/sites/realspin/2015/05/18/privacy-concerns-about-verizon-aol-deal-are-really-concerns-about-increased-competition/>.

First-party Online Service. The proposed rule should have two components regulating the tracking activity of edge providers providing a first-party online service, meaning, with respect to a particular network interaction by a particular consumer, an online service with which a consumer is intentionally interacting (e.g., a website an Internet user visited). First, an edge provider providing a first-party online service should be prohibited from requiring a consumer to consent to tracking as a condition of accessing the content or services of that edge provider. Second, when an edge provider providing a first-party online service receives a “Do Not Track” Request, the provider should be prohibited from selling, sharing, or otherwise transferring the personal information of the consumer to any other entity, including, but not limited to, a third-party online service.

Third-party Online Service. The proposed rule should require edge providers providing a third-party online service, meaning, with respect to a particular network interaction by a particular consumer, an online service that is not a first-party online service, to honor “Do Not Track” Requests. Any edge provider providing a third-party online service that receives a “Do Not Track” Request associated with a particular consumer should be prohibited from tracking that consumer’s personal information.

Remedies and Penalties. The proposed rule should contain provisions providing damages to consumers who suffer injuries from violations and subjecting edge providers to penalties for violations.

VI. CONCLUSION

If broadband and Internet users’ privacy is to be protected there must be clear, enforceable rules. Consumers currently have no way of knowing for sure if their “Do Not Track” Requests are being honored. The only solution is the adoption of enforceable rules that require edge providers to honor “Do Not Track” Requests, with meaningful remedies and penalties if

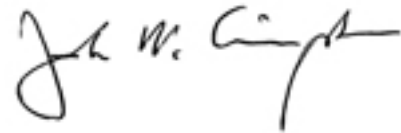
broken. As set forth above, the Commission has the authority to enact such a rule and enforce it. This, combined with the anticipated robust CPNI rules covering broadband Internet access providers, would ensure consumer privacy is protected in a meaningful way, almost certainly increasing use of broadband and the Internet.

For all of the foregoing reasons, Consumer Watchdog hereby petitions the Commission to initiate a rulemaking proceeding to require edge providers to honor users' "Do Not Track" requests.

Respectfully Submitted,

CONSUMER WATCHDOG

By:



John Simpson

Privacy Project Director

By:



Laura Antonini, Esq.

2701 Ocean Park Blvd., Ste. 112
Santa Monica, CA 90405
Telephone: (310) 392-0522
Facsimile: (310) 392-8874

Counsel for Consumer Watchdog

Dated: June 15, 2015