



network providers should even be collecting this information in the first place, particularly in the case of the content of users' communications.

A number of comments advocated industry self regulation to protect online privacy, yet failed to demonstrate that the market for Internet access is sufficiently competitive to prevent abusive behavior. In fact, recent events have proven that network providers are not at all constrained by the broadband market and will happily invade their users' private and confidential communications if it will increase their bottom line.

Several comments supported a balancing of user privacy rights with the content-driving benefits of online behavioral advertising. Each of these comments failed to recognize that web-based behavioral advertising (e.g., Google AdSense) is fundamentally different from network-based systems (e.g., NebuAd) and that the benefits of content subsidization are clearly not present with the latter. Network-based systems invade users' privacy and undermine a vital source of funding for content publishers' without providing any benefit for users or the Internet at large.

Other issues, such as Deep Packet Inspection ("DPI") and content filtering, were raised in various comments with little to no discussion of privacy. These technologies operate through the wholesale monitoring of all users' Internet communications and have far-reaching implications for users' privacy rights. DPI and content filtering constitute a form of online "wiretapping" and cannot be addressed in a vacuum.

Finally, the California Public Utilities Commission ("PUC") recommended that the Commission initiate a new proceeding to specifically address broadband privacy. Data Foundry fully supports this proposal. Online privacy is an incredibly important issue for the future of the Internet and is likely too great a topic than can be handled as a subpart of this proceeding.

**I. An effective national broadband plan must address the fundamental privacy threats posed by Deep Packet Inspection and network monitoring.**

Various comments discussed broadband privacy as though it were an issue limited to only matters of data retention and third party access.<sup>1</sup> While these are important considerations, looking at privacy through this limited lens ignores the more pressing and fundamental question of whether these parties should even collect this private user information in the first place. The best way to protect American Internet users' privacy is to ensure that their personal communications and information stays out of the hands of other parties, except when absolutely necessary.<sup>2</sup> Establishing data security rules alone would only be a band-aid solution to the underlying problem, which is that too much private user information is monitored and collected on the Internet.

In recent years, network providers have begun monitoring their users with DPI. As noted in Data Foundry's original comments, DPI is essentially an Internet "wiretap" that inspects the content of users' communications, including those that are private, confidential and/or privileged. DPI is highly divisive and its use has spurred a number of high-profile controversies domestically and abroad.

The use of DPI to monitor users is at odds with Americans' reasonable expectations of privacy in their online communications. Courts have continually recognized that users' communications are confidential precisely because the Internet has traditionally been assumed to

---

<sup>1</sup> See Comments of Cox Communications at 11-12, National Association of State Utility Consumer Advocates at 70, United States Telecom Association at 28, and Verizon and Verizon Wireless at 57.

<sup>2</sup> Certain information must necessarily be inspected by network providers to perform their routing functions, but this does not include the content of communications. In this respect, Internet communications are much like traditional mail and telephone communications, in which envelope information (or dialed telephone numbers) is considered public and letter content (or telephone audio content) is deemed to be fully private and confidential. This analogy has translated successfully to online communications, as it has allowed courts to distinguish between routing information and unseen content. See *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996). With DPI, however, this distinction fades as the content of communications becomes part of the "seen" information. DPI now threatens the legal basis for confidentiality and privilege in our online communications.

be a medium free from third party monitoring.<sup>3</sup> This recognition has led to the further finding that online communications are legally confidential and privileged, which has, in turn, enabled the Internet to become a critical tool for free expression and commerce.<sup>4</sup>

With the adoption of DPI, the benefits of a private and confidential Internet disappear. The network providers, however, seem to believe that they are entitled to inspect, collect, and utilize the private communications of their users, even though those users have always expected otherwise. By suggesting that the Commission need only address what rules apply when private information is in their hands, the network providers are essentially asking the Commission to sanction their use of DPI in all circumstances and for all purposes.

## **II. Industry self regulation will not protect Internet users' privacy because the broadband market is not sufficiently competitive to prevent abuse.**

Several comments touted industry self regulation as the best method for protecting users' online privacy.<sup>5</sup> This argument, however, rests on the assumption that there is a functioning and competitive broadband access marketplace. This assumption is not based in reality as most American Internet users have only one or two options available for unrestricted broadband access. This is not a free and functioning marketplace that is capable of restraining bad behavior through sufficient competition and the exercise of customer choice.

In recent years and under a self regulatory framework, broadband network providers have proven that the current state of competition is not enough to ensure best practices and protect users' privacy. The NebuAd controversy exposed over a dozen network providers that had allowed an outside third party to place DPI technology on their networks for the purpose of

---

<sup>3</sup> See *United States v. Heckenkamp*, 482 F.3d 1142, 1147 (2007).

<sup>4</sup> See *In re Asia Global Crossing, Ltd., et al*, 322 B.R. 247, 256 (2005).

<sup>5</sup> See Comments of AT&T at 57-59; Comcast Corporation at 26; Competitive Enterprise Institute at 7-8; Cox Communications at 11-12; Independent Telephone & Telecommunications Alliance at 24; Time Warner Cable, Inc. at 25; United States Telecom Association at 28-29; and Verizon and Verizon Wireless at 57-58.

monitoring their customers' communications. For the network providers, it was all too easy to sell off their customers' private communications because they had little fear of mass customer defection. The advertising revenues from NebuAd justified the sacrifice of their users' privacy and there is no reason to think that continued self regulation would ever lead to a different result.

Network providers are acutely aware of the practices of their local competition and the service of each often mirrors the other. When one imposes anti-consumer terms of service on their users or lets their broadband product stagnate, the other sees this as an opportunity to do the same. This became painfully obvious when Time Warner Cable announced its plans to institute extremely low and punitive usage caps on its broadband service in four markets. In each of the four cities in which these caps were to go into effect, the competing phone company (AT&T or Frontier) was already in the process of introducing usage caps themselves. Time Warner Cable knew that their customers in these cities had no other uncapped broadband options available and it took this opportunity to unfairly price gouge. Only when threatened by Congressional investigation and federal legislation, and not market competition, did Time Warner Cable (temporarily) withdraw its plans to cap and meter its broadband product.

Without a functioning and competitive broadband marketplace, self regulation will never be sufficient to protect privacy. Enforceable privacy guidelines are needed to ensure that network providers respect their customers' expectations of privacy, even when faced with a financial incentive to do otherwise. The Commission must not defer to a marketplace that has already proven itself to be incapable of safeguarding the fundamental privacy rights of American Internet users.

**III. Network-based behavioral advertising requires greater privacy safeguards than web-based behavioral advertising because it harms content publishers and is overly invasive of user privacy.**

Internet users tolerate online advertising because they understand that it financially subsidizes the online content that they enjoy. Just as with television and radio commercials, as well as newspaper and magazine print ads, users accept the inconvenience of online advertising as the “cost” of the rich world of online content. From the perspective of consumers, advertising in general is a necessary evil that facilitates cheap or free content and is not a benefit in and of itself. Content subsidization, however, only works when the content producers are compensated for their work and actually receive a share of the advertising revenues.

A number of comments addressed this benefit of content subsidization as a necessary consideration for any privacy analysis of behavioral advertising.<sup>6</sup> Insofar as those comments go, they are correct that the harms to user privacy need to be balanced against the content-driving benefits of online behavioral advertising. This is the approach that was taken by the Federal Trade Commission<sup>7</sup> and that was recently advocated by the House Subcommittee on Communications, Technology & the Internet. These comments, however, did not recognize that there are essentially two distinct forms of online behavioral advertising and each presents a very different balance between privacy and content support.

The first type of online behavioral advertising is the various web-based systems that most users are familiar with, such as Google AdSense. Content publishers employ web-based advertising networks within their web sites and are generally reimbursed based on the number of

---

<sup>6</sup> See Comments of the Chamber of Commerce of the United States of America at 8; Competitive Enterprise Institute at 7; United States Telecom Association at 28-29; and Verizon and Verizon Wireless at 62.

<sup>7</sup> See *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, February 2009 (“In developing the proposed Principles, staff attempted to balance the privacy concerns raised by online behavioral advertising against the potential benefits of the practice. Consumers have genuine and legitimate concerns about how their data is collected, stored, and used online. They may also benefit, however, from the free content that online advertising generally supports...”).

ad clicks or page views. Web-based behavioral advertising systems often utilize “cookies” to track users across the advertising network and thereby constructing a behavioral profile. For users that are not comfortable with this system, they have the option of disabling “cookies” within their browser, regularly purging their “cookies,” or employing any number of third party browser add-ons to prevent tracking and profiling.<sup>8</sup>

For web-based behavioral advertising, striking a balance between user privacy and content subsidy is entirely appropriate. Most content producers, whether professional news organizations or independent blogs, depend upon this advertising revenue and would be hard-pressed to continue offering content without it. Users have an incentive to tolerate the relatively mild invasion of their privacy because they benefit from an ad-supported web.

The second type of online behavioral advertising is network-based systems, which operate on broadband providers’ physical networks, such as NebuAd, Phorm and Front Porch. Network-based systems use DPI to monitor user behavior and insert ads into the communications as they travel the network. This type of advertising through monitoring is tremendously invasive as it surveils *everything* that users do on the Internet, rather than just tracking certain in-network websites visited. Because DPI is performed on the local broadband provider’s network infrastructure, in-between the Internet and the user, the user has no means to avoid the monitoring or the advertising.

Compounding the problem, network-based behavioral advertising provides *zero* content-subsidizing benefits. Content producers receive no advertising revenue from network-based systems. The publishers are cut out of the equation because the advertising is done entirely on the network through intercepting the communication. The broadband providers – whom do

---

<sup>8</sup> See e.g., *Add-Ons For Firefox: Privacy and Security*, <https://addons.mozilla.org/en-US/firefox/browse/type:1/cat:12> (Targeted Advertising Cookie Opt-Out (TACO) 1.8, Better Privacy 1.29, Ad Hacker 0.7, and Cookie Safe 3.0.5).

receive the advertising revenue that would otherwise support the content publishers – are exploiting their advantageous position as the man-in-the-middle to insert ads just prior to delivering the content.

Additionally, network-based advertising has a very clear negative effect on Web content because it moves the advertising revenue that the content publishers depend on to the network provider middlemen. The existence of network-based systems that compete with web-based systems dilutes the value of the traditional and beneficial web-based advertising. Any ad revenue that the network-based systems generate is necessarily at the expense of the content producers.

Furthermore, it is very probable that some network-based systems actually replace web-based advertisements with their own, essentially rendering the web-based system useless (it was believed that NebuAd operated in this manner). Graphically removing and replacing web-based ads is the likely procedure for these systems because web pages generally do not contain a great deal of unused space and the only natural location available to place an ad that will not disrupt the presentation of the web page is where the original ads reside. Clearly, if web-based ads are subject to arbitrary deletion and replacement by the network providers, the practice of web-based advertising loses its value and content producers lose their sole source of revenue.

To date, the policy debate regarding online behavioral advertising has not recognized this critical distinction between web-based and network-based systems. Comments in this proceeding have conflated the two and generally regarded each method as one and the same.<sup>9</sup> In fact, one

---

<sup>9</sup> Verizon, to its credit, has recognized that web-based and network-based behavioral advertising are in fact distinct and separate systems. *See* Comments of Verizon and Verizon Wireless at 59-60. Verizon, however, concluded that the differences between these two forms of behavioral advertising did not support separate privacy standards because the end product is not noticeably different for users. Such a conclusion totally fails to recognize the parasitic effects of network-based advertising on the web or the excessive invasion of users' privacy. Users are defenseless against network-based systems because they have no means to avoid DPI. Also, network-based advertising dilutes (or potentially destroys) the value of the web-based systems that subsidize web content, which would lead to the availability of less content. In these regards, Verizon is incorrect and network-based behavioral advertising has significant negative consequences for users that web-based systems do not.

participating party confused the nature of network-based behavioral advertising to such an extent, that its comments argued that online content publishers profit from the use of DPI:

Importantly, behavioral advertising fueled by deep packet inspection has the potential to deliver significant benefits to consumers.<sup>18</sup> Advertising is a primary source of revenue for tens of thousands of online publishers of all sizes, and more robust behavioral targeting techniques may allow original content creators to better monetize their content.<sup>19</sup> This means more free content online and fewer “paywalls.”<sup>10</sup>

For all the reasons previously stated, this cannot be. Behavioral advertising fueled by DPI provides absolutely no revenue for online content publishers because the network providers have replaced them in the advertising process.

In addressing online behavioral advertising, the Commission must not make this same mistake or confuse these two very different forms of online behavioral advertising. The Commission should seek to strike a balance between the privacy harms and the content supporting benefits of these systems separately. In so doing, the Commission must recognize that there continues to be a place for web-based systems because they provide the essential funding that keeps many content producers going. In light of the limited privacy effects of web-based systems, the content subsidizing benefits justify maintaining this practice.

Network-based systems conducted through DPI, on the other hand, are exceedingly invasive of user privacy and provide no such benefits of content subsidization. In fact, network-based systems threaten to usurp web-based systems and deprive online content producers of their only source of revenue. This danger, with no related benefits for users, requires that much greater scrutiny be applied to network-based systems and that the practice only be allowed in instances of express and informed opt-in consent. Network-based behavioral advertising and DPI should not be imposed upon users as a mandatory condition of service. Users must have the right to

---

<sup>10</sup> See Comments of the Competitive Enterprise Institute at 7.

decline these practices and still receive equivalent service. These privacy safeguards would be an appropriate and effective addition to a national broadband policy.

**IV. Commission action is needed to protect against abusive uses of Deep Packet Inspection, rather than an outright ban of the technology**

The comments of AT&T and Verizon advise that the Commission refrain from establishing privacy rules or guidelines that are specific to packet inspection technology.<sup>11</sup> These comments note the DPI has a number of legitimate network uses that do not necessarily implicate privacy concerns. They argue that calls to ban the technology would be counterproductive. AT&T and Verizon are merely knocking down a straw man, however, as neither the Commission nor other comments suggested that banning DPI would be a proper course of action. In the NOI, the Commission recognized that certain *uses* of the technology create very clear threats to user privacy. It is those uses of the technology that require Commission action to safeguard Internet privacy.

As Data Foundry explained in its original comments, the Commission should find that DPI can only be used by network providers in instances where customers have clearly and knowingly consented. Imposing DPI on users as a mandatory condition of service or refusing service to customers that do not submit to monitoring is not consensual. Requiring the use of DPI to be accompanied by adequate disclosure and user consent is entirely appropriate and is hardly a ban on the technology.

Of note, one of the most pressing difficulties in addressing the problem of DPI for the Commission will be that there is very little transparency on the issue among network providers. Very few providers have explicitly stated whether or not they use the technology. In almost all instances, it has taken scandal to expose the use of DPI. Only when Comcast was caught

---

<sup>11</sup> See Comments of AT&T, Inc. at fn 162; and Verizon and Verizon Wireless at 61.

throttling BitTorrent, did the network provider admit that it was employing the technology. The same is true of over a dozen other network providers that were found to be partnered with NebuAd. The Commission and the public should not have to wait for episodes such as these to learn who is using DPI. To fully assess and resolve the privacy threat from DPI, the Commission should seek unequivocal admissions or denials from American network providers as to whether and under what circumstances DPI is being used on their networks.

**V. Content filtering would constitute a massive violation of all Internet users' fundamental privacy rights.**

A joint filing of several members of the copyright industry – including the Recording Industry Association of America (“RIAA”) and the Motion Picture Association of America (“MPAA”) – criticized the Commission for seeking comment on and considering the inclusion of a nondiscrimination principle to the existing Internet Policy Statement.<sup>12</sup> The joint comments argued that such a policy would frustrate any attempts by network providers to filter copyrighted content from their networks. The joint comments suggested that the Commission was essentially encouraging widespread copyright infringement and, in a moment of excessive hubris, called for the Commission to publicly clarify that it is not attempting to “protect illegal activity on the Internet.”<sup>13</sup> The joint comments, however, included no discussion of privacy, which is a glaring omission considering that the comments are advocating for the wholesale monitoring and filtering of the Internet.

The joint comments of these various copyright industry organizations argue that network providers should have the ability to use “network management” techniques to enforce copyright law on behalf of content owners. This is, of course, not “network management” as a principle of

---

<sup>12</sup> See Joint Comments of American Federation of Television and Radio Artists AFL-CIO, et. al. at 3-4.

<sup>13</sup> *Id* at 5 (“As the Commission moves forward with this NOI, it should clarify that any policies or principles it recommends neither protect illegal activity on the Internet...”).

engineering. The comments have instead co-opted the term of art as a euphemism for content filtering. This is, in fact, quite the opposite of “network management” as a tool for efficiency because it implies the addition of extra layers of applications, protocols, hardware, and complexity to the network providers’ infrastructure. This new sanitized label is being used to obscure the fact that these organizations are advocating for the comprehensive monitoring of online communications with DPI.

In effect, these copyright industry groups’ arguments boil down to the proposition that all Internet users’ fundamental privacy rights should give way to copyright owners’ non-fundamental pecuniary rights. The sheer solipsism inherent in such a suggestion is astounding. No equitable balancing of rights could ever support the indiscriminate invasion of all users’ privacy in order to protect the revenues of a very small number of copyright owners. And no amount of lobbying or political clout should ever succeed in achieving such a result. The Commission must not be swayed by this argument.

**VI. The Commission should initiate a separate proceeding to address all broadband privacy issues comprehensively.**

The California PUC proposed that the Commission conduct a separate inquiry into the issues of broadband privacy.<sup>14</sup> Data Foundry fully supports this recommendation and believes that such a proceeding to identify and address the problems related to broadband privacy would be beneficial. Privacy is an extraordinarily complex issue that touches upon many aspects of broadband policy. These issues – including network inspection, content filtering, behavioral advertising, customer proprietary network information, and more – are likely too complex to be conclusively resolved as a subcomponent of this proceeding.

---

<sup>14</sup> See Comments of the California Public Utilities Commission and the People of the State of California at 29 (“Given the complexity of Internet-related privacy issues and the importance of this issue to customers and the security of the communications network, it may be best to consider any possible action by the Commission in a separate proceeding.”).

Privacy is a fundamental right that facilitates many other important individual liberties. The Internet has succeeded in part because users have always felt secure in their online activities. We know the Internet today as a medium for free expression, free exploration of ideas, and open communication because of its traditionally private nature. This privacy is now threatened by a variety of issues, which the Commission should address in one careful and comprehensive proceeding.

### **Conclusion**

This NOI's initial round of comments generated a wide variety of responses on Internet privacy. To further a full and open dialogue, these reply comments respond to a number of the arguments and proposals that Data Foundry believes would lead to inadequate privacy safeguards for the Internet. In particular, a number of comments argued that online privacy should only be addressed in the context of the broadband providers' data retention and third party access policies. Such a limited inquiry, however, would fail to deal with the more important underlying question of whether or not network providers should collect private user information in the first place. Network monitoring and unrestricted DPI are threats to online privacy in and of themselves, and rules that do not prevent such practices would fail to protect Internet users.

Many comments argued that industry self regulation will be sufficient to protect the privacy of Internet users. These comments forget that a self regulatory environment has failed to safeguard user privacy in several very high profile instances. Self regulation will continue to be insufficient to protect Internet privacy because there is not a competitive market for broadband Internet in America. Not until there is adequate competition will network providers be restrained

from violating the privacy rights of their customers. In the meantime, privacy safeguards are needed to ensure that users' private communications and information remain protected.

A number of comments addressed the need to balance user privacy with the benefits of online behavioral advertising. While this balance makes perfect sense for web-based systems, the comments failed to distinguish the more harmful network-based systems. Network-based behavioral advertising (e.g., NebuAd) is much more invasive than web-based advertising, and it produces no benefits of content subsidization. For network-based advertising, the balance between the privacy harms and the content-driving benefits is entirely one-sided. The Commission must recognize that network-based advertising presents a threat to user privacy as well as to web content publishers and ensure that this practice is not employed abusively.

Other comments extolled the benefits of DPI and advocated for content filtering with little to no discussion of the privacy issues that are implicated by these technologies. DPI and content filtering are essentially Internet "wiretaps" that operate through the wholesale monitoring of users' online communications. Any examination of such technologies requires that privacy implications be taken into account. DPI and content filtering should be employed in very limited situations and only with the express, voluntary, and informed consent of users.

Finally, the California PUC has suggested that the Commission initiate a new proceeding to address broadband privacy. Data Foundry fully supports this proposal. Privacy is an incredibly important and complex issue that touches all users of the Internet. Establishing a meaningful policy and adequate broadband privacy protections will require a tremendous amount of dialogue and public participation.

Respectfully Submitted

Matthew A. Henry  
1250 South Capital of Texas Highway  
Building 2, Suite 235  
West Lake Hills, Texas 78746  
512.888.1114  
[henry@dotlaw.biz](mailto:henry@dotlaw.biz)  
*Counsel for Data Foundry, Inc.*

July 21, 2009