



Data Foundry, Inc.  
1044 Liberty Park Dr.  
Austin, Texas 78746  
Tel: (512) 684-9700

<http://www.datafoundry.com>

January 22, 2010

*FILED ELECTRONICALLY*

Ms. Marlene H. Dortch  
Office of the Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, D.C. 20554

Re: Comments – NBP Public Notice #29  
GN Docket Nos. 09-47, 09-51, and 09-137

Dear Secretary Dortch:

Data Foundry welcomes this opportunity to provide comments on the important topic of Internet privacy and is encouraged that the Federal Communications Commission (“Commission”) is specifically addressing this issue in the National Broadband Plan. Data Foundry is a data center company that provides managed Internet, collocation, and disaster recovery services. We have long been an advocate for Internet privacy and have raised the issue in various proceedings before the Commission. As a data center company, we are intimately familiar with the issues of communications privacy and information security, and hope to provide useful assistance to the Commission in these areas.

In the National Broadband Plan Notice of Inquiry (“NOI”), the Commission asked a number of privacy questions related to this public notice. Data Foundry addressed many of those issues in our comments and reply comments. In those submissions, we explained the threats to online privacy rights posed by wholesale network inspection and called on the Commission to declare a public policy against terms of service that impose network inspection upon users *without their consent*. In examining the privacy issues raised in this public notice, we would ask that the Commission also look to those submissions for guidance.

In these comments, we will explain the distinction that needs to be made between the matters of network privacy and Web privacy.<sup>1</sup> The Center for Democracy & Technology’s (“CDT”) letter raised a number of important privacy issues but failed to

---

<sup>1</sup> While we use the term “Web” for simplicity’s sake, we are really referring to any application or service offered over of the Internet. When we use the term “network,” we are referring to the transmission facilities and physical infrastructure, generally the last mile, offered by Internet Access Providers.

draw this important distinction. The physical network and the Web are subject to entirely different levels of competition, user expectations of privacy, and monitoring capabilities. Because of these dynamics, network privacy and Web privacy should not be conflated and the Commission should not try to apply a one-size-fits-all analysis for both.

For example, most Internet users fully understand that to make an online purchase, say at Amazon.com, they will need to provide their credit card information to Amazon, but they likely do not understand that, if they are being subjected to network inspection, they are also disclosing that information to their Internet Access Provider (“IAP”). In this scenario, we can assume that Amazon will have this credit card information and privacy issues of data security, third party access, and retention policies are appropriate. For the IAP, however, the question of whether this information should even be obtained through network inspection in the first place is much more important.

## **I. Web Privacy Considerations<sup>2</sup>**

On the Web, the market for content and services is vibrant. Healthy competition provides users with many options to get their information, to engage in e-commerce, and to communicate with others. This allows consumers to vote with their mice and to pick winners and losers through exercising choice. Web content and service providers compete with each other to give users what they want in a virtual marketplace by meritocracy. This competition also curtails abusive behavior and by allowing users that are unhappy with specific privacy practices to turn to better options.

When users provide private information to a Web content or service provider, they generally understand the disclosure they are making. If, for instance, a user chooses to use Gmail, they understand that the content of their communications will be inspected and used to create behavioral advertising. When a user submits their credit card information or social security number to a website, they understand that they are giving that information to that website operator. In this regard, users truly have control over how their private information and communications are disclosed on the Web. In each case, importantly, the disclosure has been voluntary and, thus, appropriate privacy considerations are issues of third party access and data retention policies.

The one instance where users may not fully understand the privacy implications of their actions on the Web is with behavioral advertising. Behavioral advertising services use “cookies” to track users’ whereabouts across a network of affiliated websites. While users understand that they are disclosing their presence to each

---

<sup>2</sup> We note that, while Web privacy and the practices of website operators may be appropriate topics for establishing policy for the National Broadband Plan, in practice, Data Foundry believes that these are issues squarely within the province and authority of the Federal Trade Commission.

individual website, they likely do not know the extent to which that information will be aggregated to create an individual profile. There are, importantly, a number of self-defense measures that users can take to protect their privacy from this type of tracking. First, users can set their browsers to not accept “cookies” or they can purge their “cookies” on a regular basis. Also, privacy-minded users can download a variety of browser “add-ons” that will protect their privacy against this type of tracking and behavioral advertising.

All of these dynamics specific to the Web raise a variety of privacy considerations. Rules that are appropriate for website operators should be tailored to their situation and interaction with users. For Web-based behavioral advertising, there are other considerations and privacy implications. But, in each case, the information has been knowingly and voluntarily disclosed.

## **II. Network Inspection Poses a Significant and Unique Threat to Users’ Privacy Rights.<sup>3</sup>**

Network inspection, performed by IAPs through Deep Packet Inspection (“DPI”), presents a number of significant and unique privacy dangers because it involves *involuntary* disclosure. It should not be assumed that network inspection can be dealt with in the same manner as Web-based privacy issues. To try to create a common set of guidelines and policies for each would be a mistake.

DPI is essentially an Internet “wiretap.” It monitors the entirety of a users’ Internet traffic by intercepting and accessing the content of users’ communications. This wholesale inspection sees everywhere a user goes, everything a user says and to whom, and everything a user does online. With DPI, users no longer have an expectation of privacy in anything they do on the Internet because they are making a knowing disclosure of every single packet they send and receive. Privacy rights, such as the protection of privileged communications and trade secrets, can no longer be maintained in the presence of DPI.<sup>4</sup>

A helpful analogy for the implications of DPI is a monitored work network. Employees that are subject to workplace Internet monitoring cannot maintain a reasonable expectation of privacy because they understand that their employer has access to their communications. When using monitored work networks, employees have no privacy rights because they have no privacy from their employer. This is

---

<sup>3</sup> Because IAPs’ network-based practices deal with network facilities and the transmission of communications, Data Foundry believes that these issues fall squarely within the province and authority of the Federal Communications Commission.

<sup>4</sup> For a full explanation of the threat that DPI poses to users’ online expectations of privacy and legal privacy rights, see Data Foundry’s initial comments in the National Broadband Plan NOI (Docket No. 09-51).

precisely the threat posed by DPI monitoring. The public Internet will afford no expectations of privacy and users will lose all of their privacy rights.

Because DPI can be a tool for monetizing Internet traffic, IAPs have a powerful incentive to engage in network inspection. This puts the IAPs interests in direct conflict with the privacy interests of their users and, as we have seen recently, it is generally the IAPs' interests that win out. For example, in the NebuAd fiasco, it was all too easy for over a dozen IAPs to invade their users' privacy for the promise of behavioral advertising revenues.

The primary reason that network inspection and DPI pose a significant the threat to user privacy is the lack of competition in the Internet access market. Most users have only two options available for Internet access, their telephone company or their cable company. This lack of competition means that IAPs can impose highly unpopular business practices on their customers without fear of retribution through defection. Users have to get to the Internet and, essentially, have to take it no matter how abusively it is offered to them.

Because DPI involves the wholesale and involuntary inspection of users' communications, and because there is no effective competition in the Internet access market, privacy standards unique to this threat should be adopted. As Data Foundry has explained in its initial National Broadband Plan comments, we believe that DPI need not be banned, but it should only be allowed when users knowingly consent to its use and are offered a non-inspected alternative. We have called upon the Commission to issue a public policy statement against the compulsory use of network inspection, which users would be empowered to enforce themselves in courts of law. This would be a just and effective way of preserving users' Internet privacy rights, and would ensure that IAPs are held accountable when they invade their users' privacy without their permission.

### **III. Conclusion**

In addressing the important privacy issues raised in the National Broadband Plan NOI and in CDT's letter, Data Foundry urges the Commission not to attempt to apply a one-size-fits-all analysis. Network inspection through DPI poses a significant threat to Internet users' expectations of privacy and should be addressed in a manner that is tailored specifically to the problem. Data Foundry requests that the Commission recognize a public policy against nonconsensual network inspection, which users can enforce themselves. Such a public policy would provide meaning protection for online privacy that is neither overly regulatory nor dependent upon unaccountable self-regulation.

Respectfully submitted,

Matthew Henry  
1250 South Capital of Texas Highway  
Building 2, Suite 235  
West Lake Hills, Texas 78745  
512-888.1114  
[henry@dotlaw.biz](mailto:henry@dotlaw.biz)  
*Counsel for Data Foundry, Inc.*