Before the
United States Department of Commerce
National Telecommunications and Information Administration
Washington, D.C.

In the Matter of	)	
	)	Docket No. 100402174-0175-01
Information Privacy and	)	
	)	RIN 0660-XA12
Innovation in the Internet Economy	)	

COMMENTS OF DATA FOUNDRY

Data Foundry, Inc. ("Data Foundry") respectfully submits these comments in response to the National Telecommunications and Information Administration's ("NTIA") Notice of Inquiry ("NOI") released April 23, 2010.

Introduction

Data Foundry is a global provider of managed Internet, enterprise data center, collocation and disaster recovery services. Data Foundry is headquartered in Austin, Texas. We have long been an advocate for Internet privacy and we welcome the opportunity to comment in this proceeding. In the NOI, the NTIA specifically posed a number of Internet privacy questions and requested comments that address the most impending dangers to Internet users' privacy.

These comments will address with particularity the looming threat to users' privacy rights posed by deep packet inspection ("DPI") and the wholesale monitoring of Internet communications by broadband providers. Monitoring through DPI is today imposed upon Americans as a mandatory condition of broadband service. These terms are offered on a take it or leave it basis and users must consent to DPI in order to obtain service. But as a matter of law, users waive all expectations of privacy when they knowingly submit their communications to the inspection of the third party broadband provider.

Data Foundry requests the NTIA and the Internet Policy Task Force establish a public policy against the compulsory waiver of privacy as a condition of receiving broadband service. This policy would be privately enforceable in courts of law and would empower Internet users to protect their own privacy. A public policy against terms of service that impose monitoring would set a default rule of privacy for the Internet, rather than the current default of no-privacy. A declaration of public policy would provide meaningful protection for user privacy and security that is neither overly regulatory nor dependent upon unaccountable self regulation.

Comments

I. The Monitored Internet

The Internet is quickly turning into a monitored network as the use of DPI has become widespread and pervasive. Over 20 broadband providers in the United States have acknowledged either current or past use of DPI. DPI vendors Sandvine and Arbor Networks alone claim over 300 worldwide customers, including 13 of the 20 largest American broadband providers. Using the same technology that forms the Great Firewall of China, broadband providers are peering into the packets that traverse their networks and are monitoring American Internet users' online activities.

Few broadband providers will freely admit to the use of DPI because the technology is highly controversial. Generally, broadband providers mask their DPI-facilitated capabilities under the euphemism of "network management." Only when faced with public outrage and political scrutiny for certain contentious network practices, such as BitTorrent throttling and behavioral advertising, have broadband providers acknowledged their use of DPI. And while those highly-publicized practices supposedly stopped, the monitoring equipment almost certainly remains in place and Data Foundry believes it is still being used to invade Americans' privacy.

DPI constitutes the wholesale monitoring of Internet users' communications. As the Federal Communications Commission has previously noted, "DPI involves examining the contents of Web browsing session, email, instant message, or whatever data the packet contains."[1] Essentially, DPI allows broadband providers to see everything that their users do on the Internet in real-time and provides the capability of acting on that information.

While offensive to many Internet users, this highly-invasive form of monitoring presents a lucrative opportunity for broadband providers to monetize the content and various forms of traffic that touch their networks. This presents a clear conflict between the business interests of the broadband providers and the privacy interests of Internet users. For the broadband providers, it is all too easy to sacrifice the privacy of their customers for the additional revenues created by DPI. This conflict between user privacy and broadband providers' profits came to a head in the NebuAd scandal. In that instance, it took a Congressional inquiry to force a number of broadband providers to stop selling private information about their users' Internet activities and Web whereabouts.

II. With Monitoring, Traditional Expectations of Online Privacy Are Lost

Packet monitoring is anathema to an Internet that has traditionally maintained users' reasonable expectations of privacy. Courts have long recognized the confidentiality of users' online communications and their associated rights of privilege.[2] These privacy rights, however, have always depended upon the assumption that Internet communications travel from party to party – and network to network – without inspection by the carriera. The Internet and online privacy law have developed in conjunction under the premise that tools like DPI are *not* used to

[1] *See* Notice of Inquiry, *In the Matter of A National Broadband Plan for Our Future*, FCC 09-31 (rel. Apr. 8, 2009) at fn 89.

[2] *See e.g. United States v. Maxwell*, 45 M.J. 406 (1996).

invade the privacy of users' traffic. This recognition of online privacy has facilitated many of the most important features of today's Internet, such as free expression and e-commerce.

Internet users today expect and depend on having privacy in their online communications. In the NOI, the NTIA explained that, "consumers must be able to trust that their personal information is protected online and securely maintained." Users communicate in confidence with their doctors and attorneys, they shop and bank online, and business users communicate trade secrets and proprietary information over the Internet. These expectations of privacy have become engrained in Internet users and have provided Americans with the confidence to embrace the Internet with great enthusiasm.

One noteworthy exception to users' traditional expectations of privacy, however, has been in situations of workplace monitoring of employees' online communications. American courts have reasoned that employees cannot reasonably expect any confidentiality when they know that their employer is monitoring their communications.[3] There can be no privacy in such an instance and any information placed on a monitored work network will be deemed to have been knowingly disclosed. This is a commonsense rule of privacy law that applies identically to other forms of communication.[4] DPI now threatens to expand the application of this rule to the Internet at large.

In an online environment of wholesale DPI, Internet users cannot maintain reasonable expectations of privacy. Just as with monitored work networks, monitored broadband provider networks are not confidential and any communications placed on such networks are public by

[3] *See e.g. Scott v. Beth Israel Medical Center, Inc. et.al.*, 17 Misc. 3d 934 (Sup. Crt. NY 2007).

[4] See Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & Tech. 2 (2007) ("The third party doctrine provides that information 'knowingly exposed' to a third party is not subject to Fourth Amendment protection because one 'assumes the risk' that the third party will disclose that information to the government. Under this test, constitutional privacy interests in information are both bright and binary. It does not matter if the information is exposed for a limited purpose, or in confidence; it matters only whether the individual should know the information was made available to another party.").

nature. Broadband providers' mandatory terms of service clearly put users on notice of monitoring, and, by consenting to these terms, users have waived their privacy rights.[5] By merely accessing these networks and subjecting their communications to DPI, users have made a knowing disclosure of their information and all privacy rights that once applied have vanished. With DPI, the traditionally confidential Internet is replaced with one that is persistently monitored and totally without privacy.

III. The Implications of an Internet Without Privacy

An online environment that is subject to monitoring through DPI and without any expectations of privacy is a fundamental change to the nature of the Internet. Whereas users could previously expect confidentiality in their personal communications, such as financial transactions and Web surfing, this information is now public and in the hands of a third party broadband provider. This is an Internet with a default *no*-privacy rule. Whatever users do online, their activities are being watched and potentially recorded. And without the traditional safeguards associated with private information, broadband providers are under no duty to protect this information and keep it out of the hands of others.

While broadband providers may reassure their customers that their private information will be used for only a limited purpose and will remain safe with the company,[6] such promises

---

[5] *See e.g.* Verizon Online Terms of Service, http://www.verizon.net/central/vzc.portal?_nfpb=true&_pageLabel=vzc_help_policies&id=TOS (last visited Jun 8, 2009) ("Verizon may, but is not required to, monitor your compliance, or the compliance of other subscribers, with the terms, conditions or policies of this Agreement and AUP. You acknowledge that Verizon shall have the right, but not the obligation, to pre-screen, refuse, move or remove any content available on the Service, including but not limited to content that violates the law or this Agreement.").

[6] *See e.g.* AT&T Privacy Policy for AT&T Yahoo! and Video Services, http://helpme.att.net/article.php?item=8620 (last visited Jun 8 2009) ("Conducting business ethically and ensuring privacy is critical to maintaining the public's trust and achieving success in a dynamic and competitive business climate. Privacy responsibility extends not only to protection of customer account information but to the privacy of conversations and to the flow of information in data form. Subsidiaries and affiliates of AT&T Inc. (the "AT&T family of companies") understand that the trust of our customers necessitates vigilant, responsible privacy protections.").

are hollow and legally ineffective.[7] This is because privacy is binary – information is either wholly private or wholly public[8] – and once that information has been inspected by a third party broadband provider, that data becomes public to all and can never again be deemed private. Thus, as with all public information, the records of users' online communications would not be subject to the protection of privacy laws and could be permissibly sold or released by the broadband provider.

A monitored Internet, without reasonable expectations of privacy, would profoundly change the way that Americans communicate. Consumers' need to maintain the confidentiality of their private information would not change and many, particularly businesses, would be left searching for other means of sending sensitive communications, such as by mail or facsimile. Data Foundry has already witnessed this effect first hand, as a number of our customers have inquired into the security of their data as it travels the Internet to our data centers. In response, we can only guarantee the security of their information once it has arrived at our facilities and are forced to admit that our customers' data is almost certainly not private and secure on the public Internet. One customer, a law firm that needs to maintain the confidentiality of its attorney-client privileged communications, has stopped using the Internet to transmit its sensitive materials altogether. The customer now burns large amounts of data to disk, which it sends by overnight delivery to our data centers. Unfortunately, as more businesses and users come to the

---

[7] *See e.g. United States v. Miller*, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities...").

[8] *See* Daniel J. Solove, *The Digital Person*¸ 143 (2004) ("The secrecy paradigm … is deeply entrenched in information privacy law. In addition to focusing on whether information is completely secret or not, the paradigm categorizes information as either public or private. When information is private, it is hidden, and as long as it is kept secret, it remains private. When it is public, it is in the public domain available for any use. Information is seen in the black-and-white manner; either it is wholly private or wholly public.").

same realization about the public nature of online communications, abandoning the efficiency and benefits of the Internet will become more common.

IV. Solution: The Protection of Privacy As a Public Policy

The destruction of all users' online expectations of privacy through widespread DPI should not be a part of America's broadband future. In helping to establish policies to protect Internet privacy, the NTIA and the Internet Policy Task Force should recognize the critical role that traditional expectations of privacy have played in the development and success of the Internet to this point. Maintaining users' privacy rights will be imperative in ensuring an open and prosperous Internet into the future. Users that want and require privacy should not be forced to submit to DPI as a mandatory condition of service and should have the opportunity to remain free from monitoring. DPI must only occur with the user's informed consent (opt-in) and actual knowledge that the result will be the total waiver of all expectations of privacy in their inspected communications. This standard of voluntary monitoring – rather than mandatory monitoring – would set privacy as the default rule for American broadband.

Data Foundry recommends that the Department of Commerce, the NTIA, and the Internet Policy Task Force mandate this rule through a simple declaration of public policy against the forced waiver of privacy as a compulsory condition of service. Such a declaration would be enforceable in courts, under traditional contract and consumer protection laws. This would empower Internet users to protect their own privacy rights by ensuring that broadband Internet access is never offered on a monitored-only basis. Should broadband providers violate this public policy and offer Internet access without a clear opt-in requirement for monitoring, it would be the consumers themselves and their state attorneys general that would bring broadband providers back into compliance.

A declaration of public policy against the non-consensual monitoring of Internet users' communications would be neither overly regulatory nor totally dependent upon faithful and honest self-regulation. The NTIA and the Internet Policy Task Force could essentially announce the policy and leave the role of enforcement with private citizens. This would relieve the federal government of the burden of *ex post* enforcement on a case by case basis and would avoid the dangers of political arbitrariness or regulatory capture. Private enforcement, rather than continuous federal regulation at multiple agencies would ensure that broadband Internet privacy is safeguarded for the future with the least administrative entanglement and the most accountability.

Conclusion

The traditional expectations of privacy associated with Internet communications have been one of the most important factors in the success of the Internet as a democratic medium. Privacy is not an end, but a means for the most fundamental of individual rights. On the Internet, privacy facilitates free expression, free exploration of ideas, free worship, and free communication with others.

Traditional expectations of online privacy have also helped to facilitate the explosion of e-commerce and the transition to a digital marketplace. It is critical for businesses that their transactions and communications remain private and free from third party purview. With reasonable expectations of privacy, businesses and consumers have learned to trust the Internet with their secret and proprietary information. With the Internet's inherent advantages of efficiency and availability of near limitless information, the online marketplace has become an integral part of America's economy.

All of these benefits of online privacy are now threatened by DPI and broadband monitoring. Unfair terms of service, offered on a take it leave it basis, require users to consent to the inspection of their communications and effectively waive their expectations of privacy. Data Foundry requests that the NTIA and the Internet Policy Task Force establish a clear public policy against broadband contracts that unfairly impose Internet monitoring upon Americans. Doing so would set a default rule of privacy for the Internet and require informed opt-in consent before users can be forced to submit to DPI. Such a public policy would provide meaningful protection for online privacy that is neither overly regulatory nor dependent upon unaccountable self regulation.

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
Counsel for Data Foundry, Inc.

June 14, 2010