Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	GN Docket No. 09-191
Preserving the Open Internet	)	
	)	WC Docket No. 07-52
Broadband Industry Practices	)	

COMMENTS OF DATA FOUNDRY

Data Foundry, Inc. ("Data Foundry") respectfully submits these comments in response to the Federal Communications Commission's ("Commission") Notice of Proposed Rulemaking ("NPRM") released October 22, 2009 (FCC 09-93).

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 online privacy and an open Internet. We welcome the opportunity to comment in this landmark proceeding on these important issues that the Commission has recognized as critical to the future of the Internet.

The NPRM requested that the public and industry participants submit comments in response to the Commission's proposed Net Neutrality rules and related issues. We at Data Foundry are generally supportive of the Commission's desire to safeguard the Internet's historically neutral, non-discriminatory nature to ensure that it remains open to all users and innovators. We believe, however, that the Commission's stated approach to "reasonable network management" will weaken the proposed neutrality rules and will authorize Internet Access Provider ("IAP") practices that destroy users' online privacy rights. Data Foundry believes that,

in order to achieve the NPRM's goals of encouraging innovation and protecting users' rights,[1] the Commission must not establish an Internet access regime of prioritization and content filtering, both of which would require pervasive monitoring of all users' communications. Instead, the Commission should adopt a definition of reasonable network management that is consistent with traditional network practices and is itself neutral with regard to content, applications, services, and devices. Additionally, disclosure of network practices that threaten user privacy, as well as the consequences of submitting to those practices, is essential to a free and open Internet and should be incorporated into the Commission's transparency rule. Data Foundry believes that these steps we propose are consistent with the fundamental principles of an open and neutral Internet.

Comments

I. The Commission's Proposed Definition of Reasonable Network Management Threatens Internet Users' Privacy Rights By Mandating Deep Packet Inspection.

Each of the NPRM's six proposed rules are subject to reasonable network management practices by IAPs.[2] The Commission explains that it wants to permit the IAPs to institute certain practices to alleviate network congestion and quality-of-service problems.[3] Included in these practices, the Commission has proposed to authorize IAPs to prioritize "managed services" and to filter for unlawful content or unlawful transfers of content.[4] These two practices, which are not traditionally considered network management functions, are of grave concern to Data Foundry because they threaten to undermine the Commission's purpose in this proceeding (each practice will be addressed in turn below) and destroy the fundamental privacy rights of Internet users.

---

1 *See In the Matter of Preserving the Open Internet Broadband Industry Practices*, GN Docket No. 09-191, WC Docket No. 07-52, Notice of Proposed Rulemaking ("NPRM") at ¶ 133.

2 *See id* at ¶ 136.

3 *See id* at ¶ 80.

4 *See id* at ¶ 139.

In order to identify specific Internet traffic for filtering and prioritization, the IAPs will need to monitor the content of all users' traffic with Deep Packet Inspection ("DPI"). This is because content, as well as applications and services, often cannot be ascertained from packet header information alone. The Commission's proposed reasonable network management rules not only authorize DPI, which is an issue still pending in the National Broadband Plan NOI proceeding,[5] but deem the use of the technology presumptively reasonable even without user consent or forewarning.

Data Foundry has previously addressed DPI and its destructive effects upon Internet users' online expectations of privacy in the Broadband Industry Practices NOI[6] and the National Broadband Plan NOI proceedings.[7] In sum, when users consent to DPI and submit their communications to content monitoring by their IAP, they are making a knowing disclosure and waiving all expectations of privacy. Essentially, the public Internet becomes akin to a monitored workplace or university network on which privacy rights cannot be maintained.[8] Users forfeit their expectations of privacy on a DPI-monitored network and previously confidential communications, such as those that are privileged or that involve trade secrets, lose their legal protections.

The Internet has developed into the great social and economic success that we know today in part because users have always maintained reasonable expectations of privacy online. Not only have users been assured of their ability to communicate in confidence but this privacy has served as the foundation for exercising their fundamental rights of free speech, free

---

[5] *See In the Matter of a National Broadband Plan for Our Future*, GN Docket No. 09-51, Notice of Inquiry ("Broadband Plan NOI") at ¶ 59.

[6] *See* Ex Parte of Data Foundry in *In the Matter of Broadband Industry Practices*, GN Docket No. 07-52, Notice of Inquiry ("Broadband Practices NOI") at Attachment (October 15, 2007) (http://fjallfoss.fcc.gov/ecfs/document/view?id=6519741393).

[7] *See* Comments of Data Foundry in Broadband Plan NOI at pp. 2-6. (http://fjallfoss.fcc.gov/ecfs/document/view?id=6520220238).

[8] *See e.g. United States v. Angevine*, 281 F.3d 1130, 1132-33 (2002).

association, and free exploration of ideas. The explosion of e-commerce has also depended upon reasonable expectations of privacy in order for businesses to transition operations online and to facilitate confidential transactions and communications. These benefits of an Internet that supports user privacy are now threatened by the Commission's contemplated mandate for wholesale content monitoring for the purposes of filtering and prioritization. These effects entirely contradict the Commission's stated goals in this proceeding of protecting consumers and empowering users.[9]

II. Enlisting IAPs to Filter the Content of Users' Communications is an Invasion of Privacy and an Inappropriate Delegation of Law Enforcement Authority to Private Parties.

In addition to the massive invasion of user privacy that content filtering would present, the Commission's enlisting of the IAPs to perform this task is wholly inappropriate. It is an astonishing proposition on the part of the Commission to argue that it would be reasonable to deputize private businesses to be the enforcers of copyright and child pornography laws. These businesses are not police agencies and are in no way suitable to be the judge, jury and executioners of civil and criminal laws. The NPRM matter-of-factly states that it would be justifiable for IAPs to take up responsibility for the enforcement of copyright laws, belying the extraordinary nature of such a suggestion.[10] It is difficult to conceive of a comparative situation in which the government would so willingly recognize a private party as having total independent authority and discretion – even beyond that available to the government – to enforce the law upon others. This kind of unrestrained and officially-endorsed vigilantism happens nowhere else in our nation and it should not begin now in this proceeding.

---

9 *See* NPRM at ¶ 53.

10 *See id* at ¶ 136.

To be clear, any enforcement of copyright laws through content filtering would be the prosecution of unlawful *acts*, not unlawful *content*. Copyrighted content is itself not unlawful, rather it is the unlicensed public performance, transfer, or copying of that content which is unlawful. So, to enforce copyright law, the IAPs would be policing criminal activities occurring online. While the NPRM cites to the Commission's Title I ancillary authority to propose these rules, it is not clear that that authority confers law enforcement powers upon the Commission over criminal acts that happen to occur online. If the Commission did have such authority, the FCC would have the power to enforce all criminal and civil laws that are violated by use of the Internet. It cannot be that the Commission has such wide-ranging law enforcement powers and, therefore, it cannot have the authority to either prosecute copyright laws or to enlist private parties to do so on the Commission's behalf.

Even if the Commission did have the authority to enforce the nation's copyright laws, conscripting IAPs to perform this function would come dangerously close to treading upon the Constitution's non-delegation doctrine.[11] Although the NPRM presents content filtering as something that the IAPs would perform independently,[12] the Commission's recognition – when no such authority has ever been established before – and official sanctioning of their right to do so could very well be considered a delegation of authority and make the IAPs state actors. Then, the monitoring and enforcement process by which content filtering was carried out – without due process or probable cause – would again call into question the constitutionality of content filtering.

That the Commission would even consider authorizing IAPs to become the enforcers of copyright law, while at the same time proclaiming its intentions to promote investment,

---

11 *See Carter v. Carter Coal, Co.*, 298 U.S. 238 (1936).

12 *See* NPRM ¶ 75.

innovation, competition and consumer protection, shows a misunderstanding of how such a regime would unfold. The IAPs, most of whom are content owners and content distributors themselves, would have an inherent incentive to over-filter and abuse their power to favor their own content offerings. In the case of video, IAPs are presented with an obvious conflict of interest. Many offer "cable" video services (whether traditional cable or IP) that directly compete with broadband content for the attention of their subscribers. These IAPs would have a clear incentive to remove any online content that threatened their cable revenues in order to force users offline. The prospect of such anti-competitive and anti-Internet practices should demonstrate why IAP-performed content filtering would be antithetical to the Commission's objectives here.

Finally, content filtering would almost certainly turn out to be a failure in practice, with little to no effect on copyright infringement. One truism to emerge from the online copyright wars of the last decade is that any attempts to combat online infringement inevitably result in the infringers becoming more sophisticated and their methods more distributed in a ceaseless game of Whac-A-Mole. When Napster was taken down, it was quickly replaced by less centralized peer-to-peer programs like Kazaa and Limewire. Once those came under fire, infringers turned to online file storage sites like Megaupload and RapidShare. And, in the most recent example, the recent demise of thepiratebay.org torrent index, did nothing to affect infringing activity, only shuttling its users to any of dozens of other similar torrent indexes. Unfortunately, any Commission effort to take up this fight will likely have the same predictable result. Those intent on infringing copyrighted works will adapt and overcome, and the only lasting effect will be wholesale monitoring of innocent Internet users with DPI and the destruction of their privacy

rights. Such a result would be incredibly harmful for users and Data Foundry urges the Commission not to authorize or mandate content filtering.

III. Mandating that IAPs Prioritize Managed Services Will Similarly Threaten User Privacy with DPI and Undermine Intended Purpose of this Proceeding.

Along with content filtering, Data Foundry is concerned with the Commission's apparent intention to establish a new priority classification of Internet traffic under the guise of "managed services." Throughout the NPRM the Commission notes that the single greatest factor in the past success of the Internet has been its open architecture that gives no preferential treatment to any applications, services, or content.[13] Now, confusingly, the Commission proposes abandoning this core neutrality principle in order to prioritize certain applications and services, such as VoIP and telemedicine, in order to "promote the goals of an open Internet."[14]

This new classification of managed services that receive preferential treatment over all other types of Internet traffic is antagonistic to the purpose of this Net Neutrality rulemaking. Instead of codifying rules that prevent preferential treatment of certain applications and services, the Commission intends to do the exact opposite by establishing an entire prioritized class of traffic. It is as though the Commission is painting over the six original proposed rules with one new disingenuous rule that reads "All bits are equal, but some bits are more equal than others."[15] Data Foundry urges the Commission not to pursue this prioritization plan as it completely undermines the purpose of this proceeding and the open Internet.

If the Commission decides to go through with the proposal to prioritize certain preferred applications and services across the public Internet, it will likely run into several insurmountable obstacles. This type of prioritization is not a new idea and has been attempted before without

---

13 *See id* at ¶¶ 3 and 56

14 *See id* at ¶ 108.

15 *See* Orwell, George. Animal Farm. London: Secker & Warburg, 1945.

great success. DiffServ and IntServ are both systems intended to prioritize traffic subsets within a user's allotted bandwidth, but these services have not gained widespread adoption due to several of features inherent to the open Internet. These same features will likely preclude the successful implementation of the Commission's prioritization plan.

The most difficult of these obstacles to prioritization is the nature of the public Internet itself. The Internet, as a network of networks, has no central authority and is subject to the discretions of the many network operators. When one network operator establishes a prioritization system, it can only ensure that priority across its own network. If it must hand traffic off to a peer, there is no guarantee that the preset priority will be maintained throughout transit across the Internet. In fact, if the other network operators that handle the traffic have implemented their own different prioritization schemes, the initial priority will almost certainly not be maintained and the original traffic runs the risk of being relegated to the non-priority lane. Were such a prioritization patchwork to take hold, the Internet would likely become less efficient and reliable than our current best efforts regime.

In order for the Commission's prioritization plan to work successfully across the public Internet, the Commission would be forced to assume responsibility as the priority-determining body and dictate its preference rankings to all network providers. Only with this imposition of a universal priority scheme would all the many networks be compelled to maintain one priority from end to end. This type of top-down prioritization would put the Commission in the position of picking winners and losers and would present a significant barrier to entry for new innovators. This intensive heavy-handed regulation, however, is exactly not what the Commission intended

its role to be in the broadband Internet market. The Commission instead has stated that it prefers a limited "light-handed regulation" that sets only "high-level rules."[16]

IV. The Commission's Concept of Reasonable Network Management Will Stifle Network Investment and Drive the Widespread Adoption of Encryption.

Data Foundry believes that the Commission's novel interpretation of network management as a practice that includes content filtering and application prioritization will have unintended consequences for users and for the Internet. The first consequence being that IAP investment in the Internet infrastructure will decrease. Filtering and prioritization will become proxies for network build outs and methods of staving off purchasing network hardware. This is a band-aid solution to a last mile network that is already suffering in many areas from neglect. Irresponsible IAPs will be tempted to continually put off network construction in favor of removing more and more user traffic under the guise of content filtering while increasingly disadvantaging non-priority traffic. Using these methods as crutches, network build outs – the preferred form of network management – will be delayed and American broadband will fall further behind other industrialized nations in both penetration and speeds.

A second consequence to the authorization of these new types of network management will come from users themselves. By authorizing the wholesale and unrestricted use of DPI by the IAPs without any privacy safeguards, users will surely take the initiative to protect their privacy rights. The Commission will be creating a market demand for effective encryption by forcing users that desire privacy to fend for themselves, and that demand will surely be met. Ubiquitous encryption is the logical and foreseeable response to a monitored Internet.

While effective encryption will be of great benefit to users that have lost their expectations of privacy due to DPI, it will frustrate a number of the Commission's objectives for

[16] *See* NPRM at ¶ 49.

the Net Neutrality rules and for the National Broadband Plan proceeding. If users insist on encrypting the entirety of their Internet traffic to be protected from monitoring, prioritized managed services will not be available to them. IAP efforts to manage congestion or monetize traffic will fail because content and application information will be hidden. And the government's national security and law enforcement efforts will also be impeded by the introduction of effective encryption technologies.

V. Disclosure of Network Practices Will Establish Users' Expectations of Privacy and Must Clearly Explain to Users the Effects of Those Practices.

The Commission also requested comment on how much disclosure should be reasonably required by the sixth proposed principle of transparency. Data Foundry wholeheartedly agrees with the Commission's belief that sunlight is the best disinfectant and that, in general, the more disclosure to the public, the better. Users and innovators must be sufficiently informed by their IAPs how their traffic is handled and what network management practices they are subjected to.

Not only is transparency critical to various technology issues, disclosure is vital to users' privacy rights, which the Commission assumed not to be the case.[17] The IAPs' disclosure of network management practices will be a determining factor as to whether users have any reasonable expectations of privacy. If this disclosure notifies the users that the content of their communications is subject to monitoring, an expectation of privacy cannot survive. Because privacy is vitally important to so many Internet users, this disclosure must be clear and comprehensible. And not only must it explain the network inspection practices, it must also explain the consequences upon the user's expectations of privacy. Most users cannot be expected to read their terms of service and immediately grasp the legal effects, so the IAP should make this clear. For example, in a recent federal criminal case, a user of Yahoo! mail was found to

[17] *See id* at ¶ 130.

have no expectations of privacy in his email communications due to Yahoo!'s terms of service.[18] These contract terms, however, were written in legalese and it is not reasonable to think that user would understand that he waived his expectations of privacy without explicit notice. For this reason, the Commission's transparency rule should require not only the disclosure of network management practices, but the legal privacy effects as well.

Conclusion

Data Foundry is supportive of the Commission's intention to preserve the traditionally open nature of the Internet and hopeful that this rulemaking process yields a wise and effective neutrality framework. We are troubled, however, by the NPRM's inclusion of content filtering and prioritization practices within the definition of reasonable network management. Data Foundry believes that these practices are unlikely to accomplish their intended results. Instead, the sanctioning of these practices will be an authorization for IAPs to conduct wholesale monitoring of their users' communications with DPI. Filtering and prioritization will constitute widespread invasions of privacy, rather than reasonable and effective network management. Only by adopting Net Neutrality rules that are not undermined at the outset by these ill-advised network practices will the Commission succeed in promoting online competition and innovation, while at the same time safeguarding Internet users' privacy.

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.

January 14, 2010

[18] *See United States v. Hart*, 2009 U.S. Dist. LEXIS 72597 at ¶¶ 51-53 (2009).